Summary-

We have observed emails from sender “Sender ID- root@rhinestone-nailheads[.]com” pretending as sender TCS HR. The email addressed to associates for viewing completed renewal application document along with grammatical content mistakes. Email contains a note that the document can be viewed only with organization email and is password protected. The link to view document is phished and is currently not found or removed.

As investigated, we found 321 emails were sent to associates with below different subjects and relevant email content (screenshots attached below in miscellaneous observation) out of which 23 were delivered. Emails with 2nd subject are found to be blank without and content while emails with 3rd and 4th subjects are quarantined in M365 Defender under Anti-Spam Policy.

1. Q4 Doc. Review, End of Year Bonus Allocation. Pls. sign and return
2. FYI
3. tcs -(1) Message Received 06:17 AM, October 18, 2023
4. Change Your Microsoft 365 Password Immediately.

Email Signature-

The email doesn’t contain any specific signature but pretended like automated email sent from company HR, HR@tcs.com with tempered image object.

Verdict-

The email found to be phishing with the motive of harvesting credential.

Action Taken-

We have blocked all malicious IOCs, sender ID and requested email deletion from user’s mailbox.

One associate has accessed phishing url on 20th Oct,2023, However, user confirmed that she had not entered credentials. Furthermore, user don’t remember whether page was accessible at that time, hence asked her to change password.

We have raised IMT for the incident- ES191239.

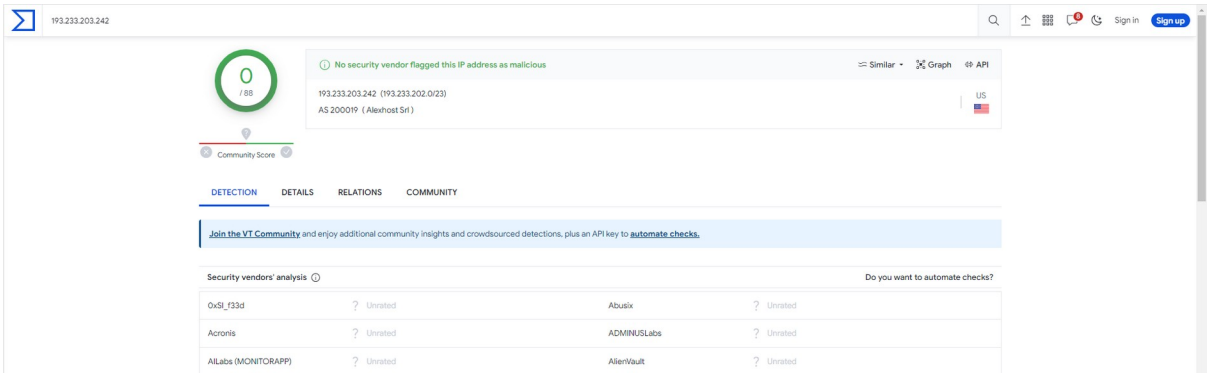
Technical Investigation

Header Analysis

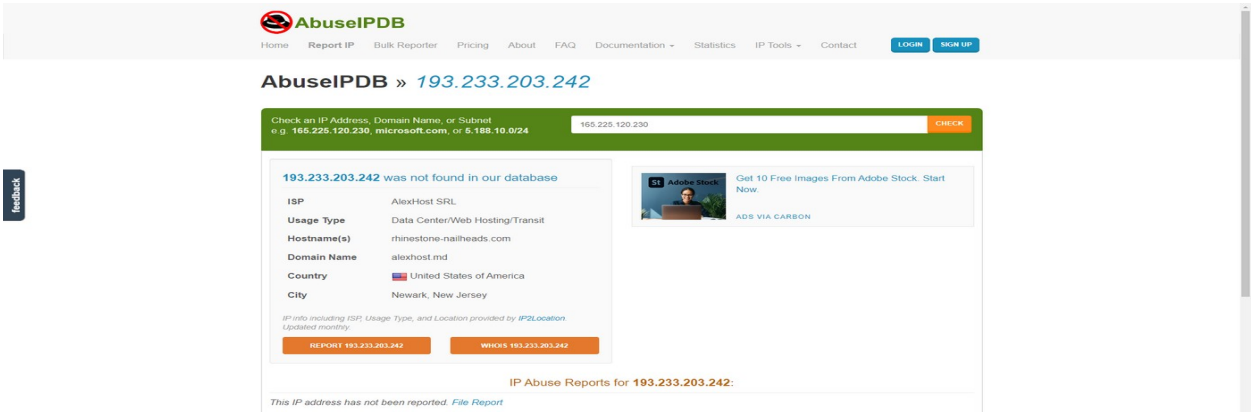
- **Sender IP- 193[.]233[.]203[.]242**

Reputation-**Non-Malicious**

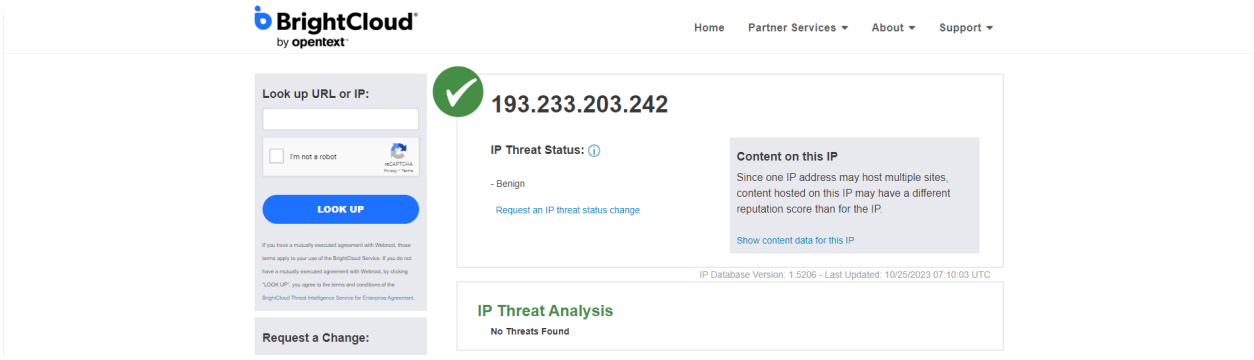
Virus Total-



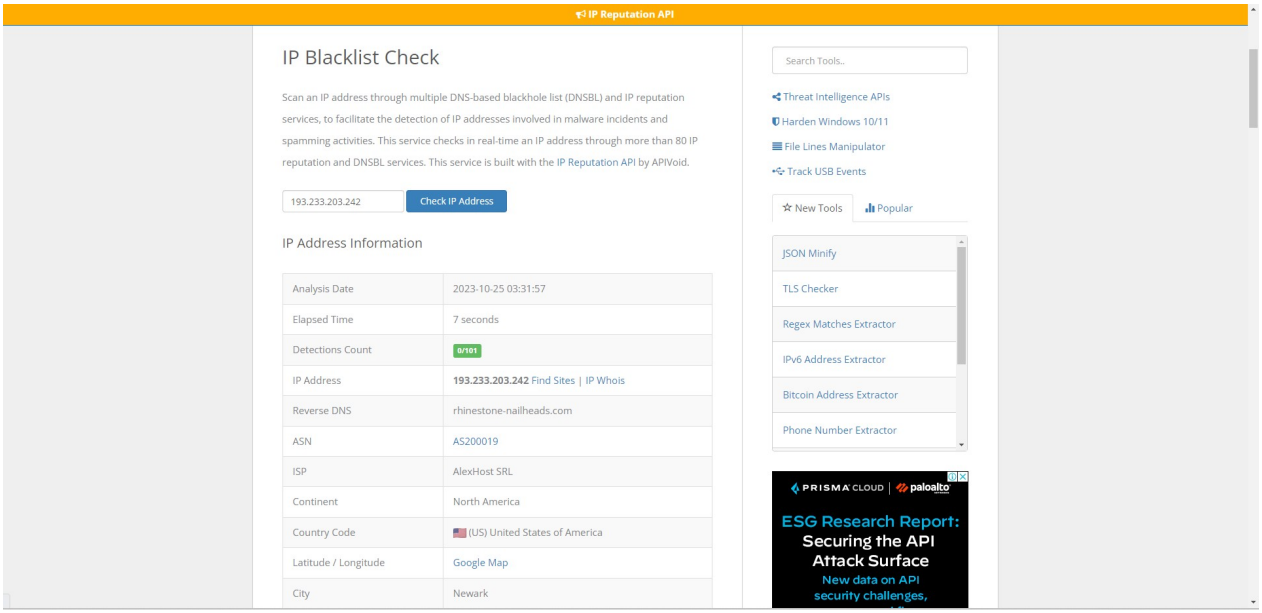
AbuseIPDB



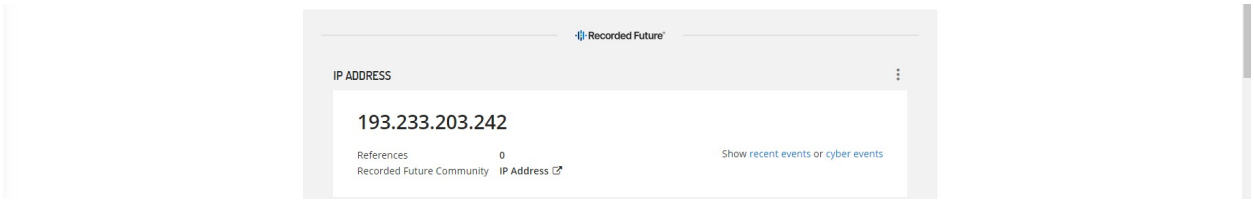
BrightCloud


BrightCloud
by opentext
Home
Partner Services
About
Support
Look up URL or IP:
I'm not a robot
LOOK UP
Request a Change:
193.233.203.242
IP Threat Status:
- Benign
Request an IP threat status change
Content on this IP
Since one IP address may host multiple sites, content hosted on this IP may have a different reputation score than for the IP.
Show content data for this IP
IP Database Version: 1.5206 - Last Updated: 10/25/2023 07:10:03 UTC
IP Threat Analysis
No Threats Found

IPVoid


IP Reputation API
IP Blacklist Check
Scan an IP address through multiple DNS-based blackhole list (DNSBL) and IP reputation services, to facilitate the detection of IP addresses involved in malware incidents and spamming activities. This service checks in real-time an IP address through more than 80 IP reputation and DNSBL services. This service is built with the IP Reputation API by APIVoid.
193.233.203.242
Check IP Address
IP Address Information
Analysis Date 2023-10-25 03:31:57
Elapsed Time 7 seconds
Detections Count 0/101
IP Address 193.233.203.242 Find Sites | IP Whois
Reverse DNS rhinestone-nailheads.com
ASN AS200019
ISP AlexHost SRL
Continent North America
Country Code (US) United States of America
Latitude / Longitude Google Map
City Newark
Search Tools..
Threat Intelligence APIs
Harden Windows 10/11
File Lines Manipulator
Track USB Events
New Tools
Popular
JSON Minify
TLS Checker
Regex Matches Extractor
IPv6 Address Extractor
Bitcoin Address Extractor
Phone Number Extractor
PRISMA CLOUD | paloalto
ESG Research Report:
Securing the API Attack Surface
New data on API security challenges,

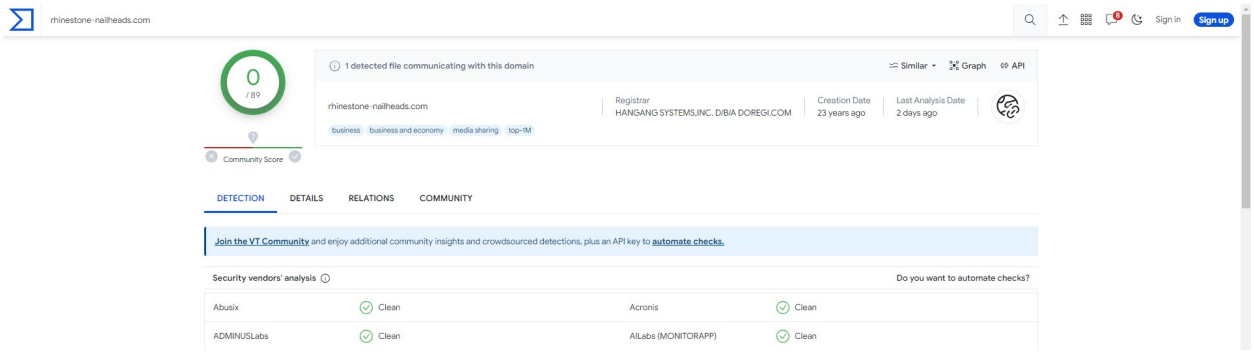
Recorded Future



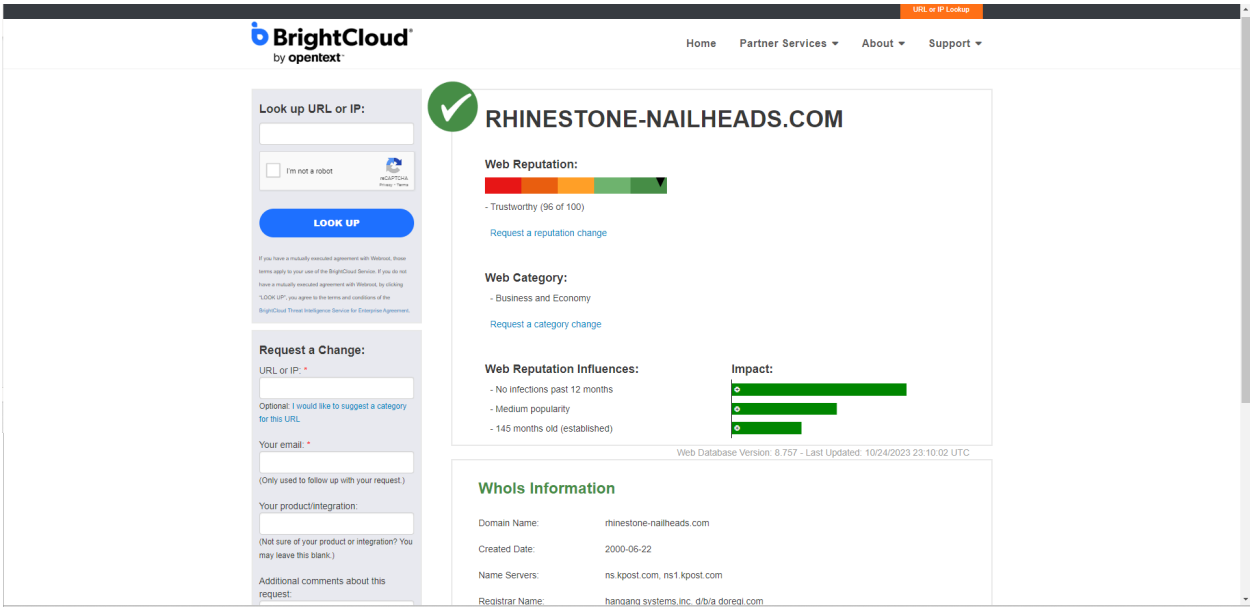
❖ Sender Domain- rhinestone-nailheads[.]com

Reputation-**Non-Malicious**

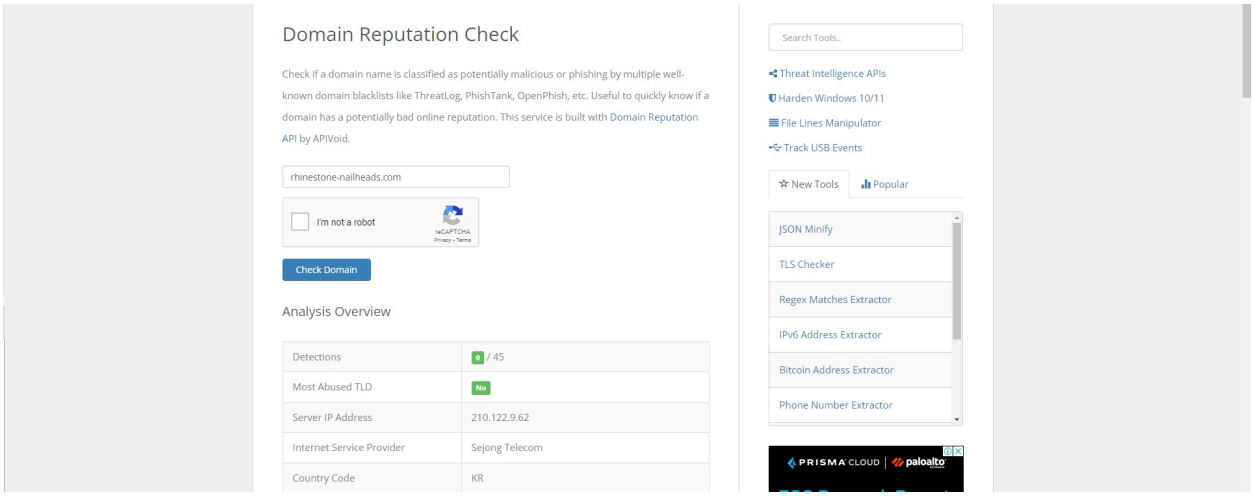
Virus Total



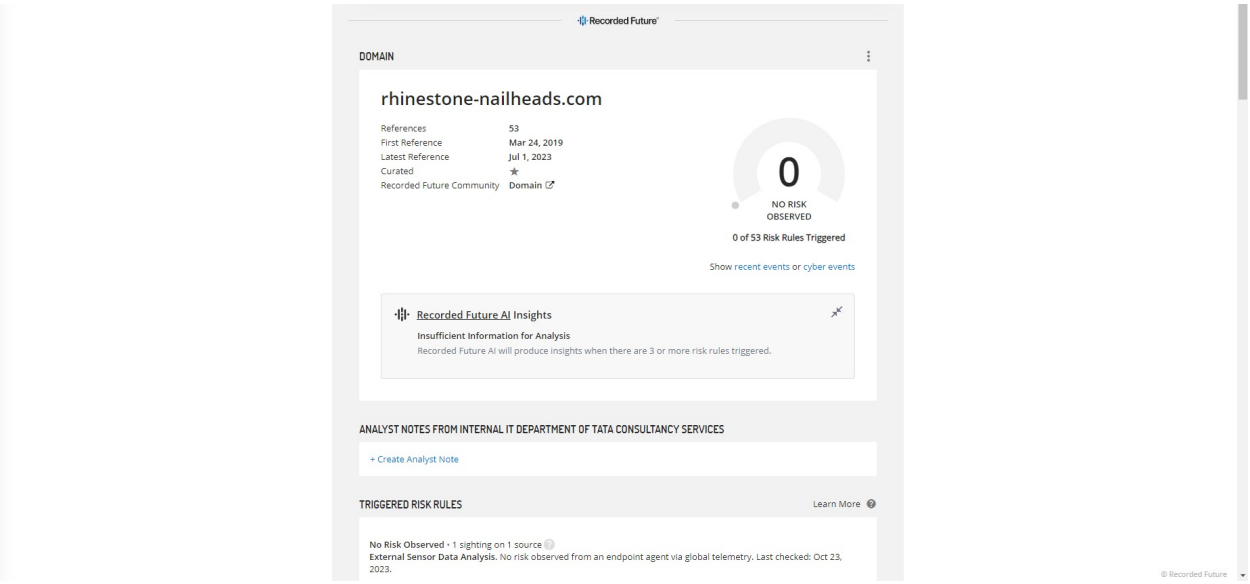
BrightCloud



URLVoid


Domain Reputation Check
Check if a domain name is classified as potentially malicious or phishing by multiple well-known domain blacklists like ThreatLog, PhishTank, OpenPhish, etc. Useful to quickly know if a domain has a potentially bad online reputation. This service is built with Domain Reputation API by APIVoid.
rhinestone-nailheads.com
I'm not a robot
Check Domain
Analysis Overview
Detections 0 / 45
Most Abused TLD No
Server IP Address 210.122.9.62
Internet Service Provider Sejong Telecom
Country Code KR
Search Tools..
Threat Intelligence APIs
Harden Windows 10/11
File Lines Manipulator
Track USB Events
New Tools
Popular
JSON Minify
TLS Checker
Regex Matches Extractor
IPv6 Address Extractor
Bitcoin Address Extractor
Phone Number Extractor
PRISMA CLOUD | paloalto

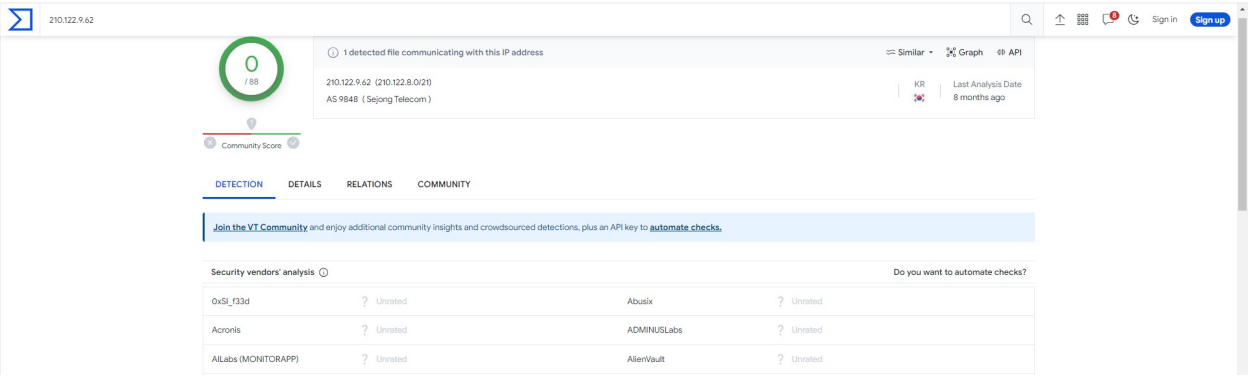
Recorded Future


Recorded Future
DOMAIN
rhinestone-nailheads.com
References 53
First Reference Mar 24, 2019
Latest Reference Jul 1, 2023
Curated ★
Recorded Future Community Domain
0
NO RISK OBSERVED
0 of 53 Risk Rules Triggered
Show recent events or cyber events
Recorded Future AI Insights
Insufficient Information for Analysis
Recorded Future AI will produce insights when there are 3 or more risk rules triggered.
ANALYST NOTES FROM INTERNAL IT DEPARTMENT OF TATA CONSULTANCY SERVICES
+ Create Analyst Note
TRIGGERED RISK RULES
Learn More
No Risk Observed · 1 sighting on 1 source
External Sensor Data Analysis. No risk observed from an endpoint agent via global telemetry. Last checked: Oct 23, 2023.
© Recorded Future

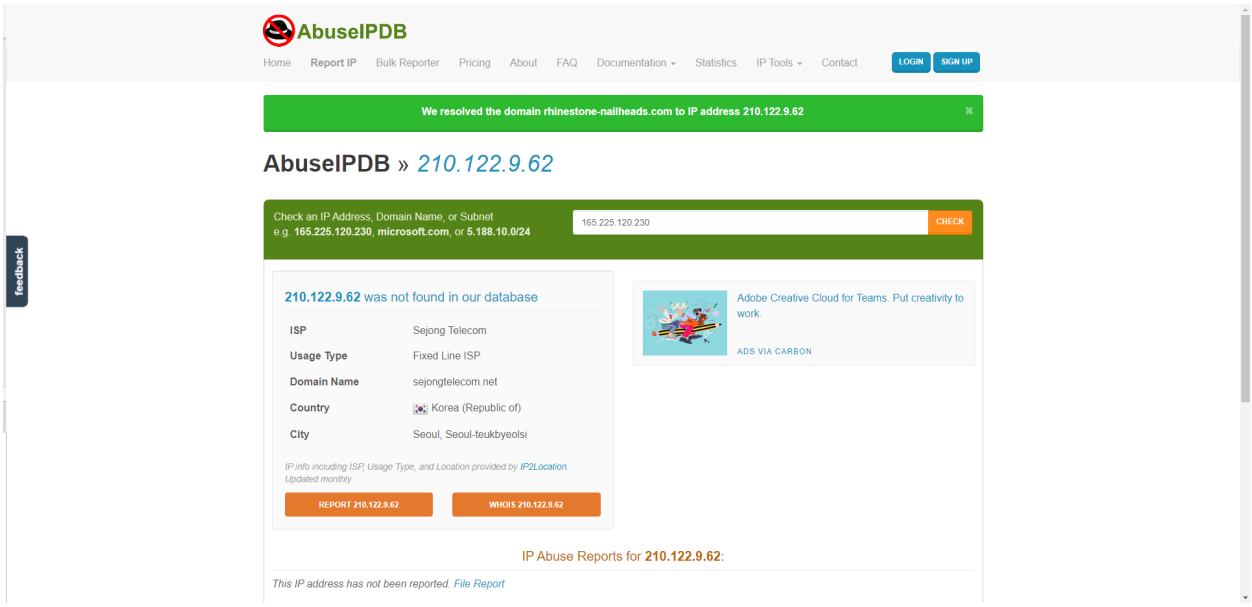
❖ Sender Domain Hosted IP-210[.]122[.]9[.]62

Reputation- **Non-Malicious**

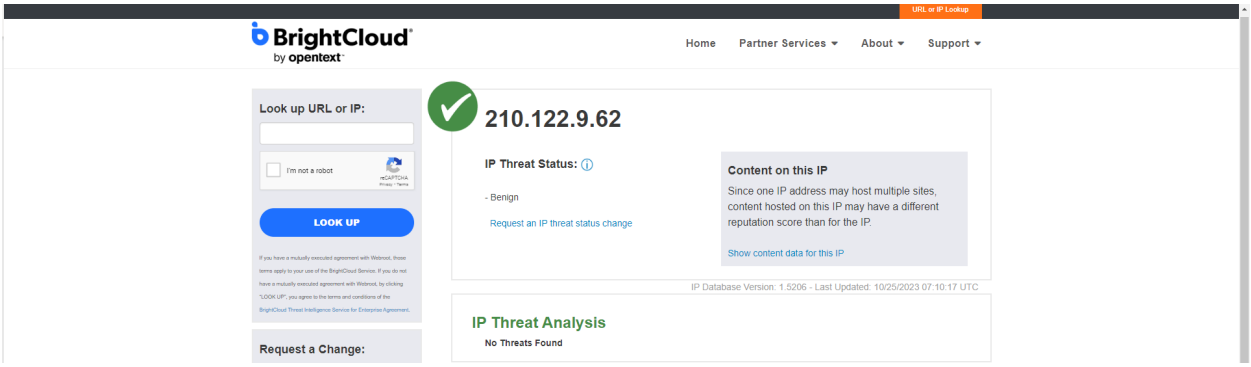
Virus Total



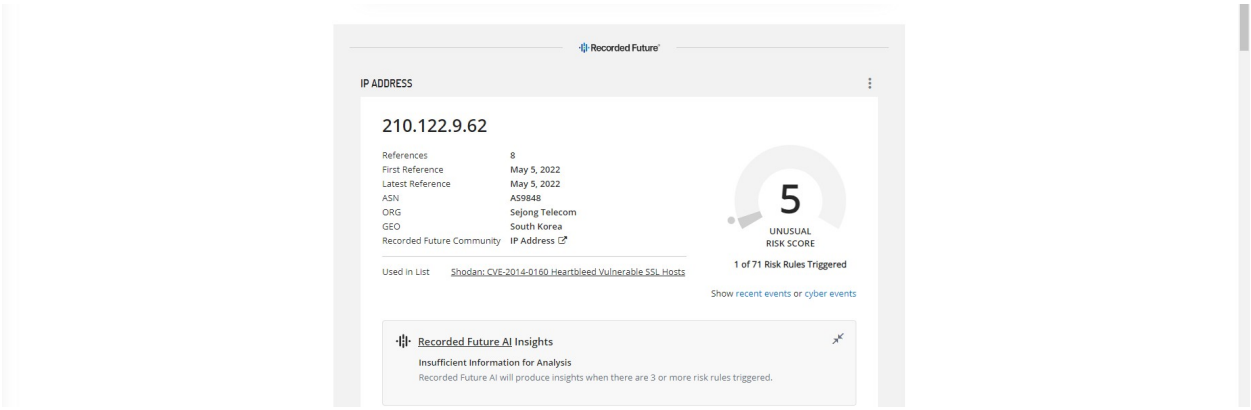
AbuseIPDB



BrightCloud


URL or IP Lookup
BrightCloud
by opentext
Home
Partner Services
About
Support
Look up URL or IP:
I'm not a robot
LOOK UP
Request a Change:
210.122.9.62
IP Threat Status:
- Benign
Request an IP threat status change
Content on this IP
Since one IP address may host multiple sites, content hosted on this IP may have a different reputation score than for the IP.
Show content data for this IP
IP Database Version: 1.5206 - Last Updated: 10/25/2023 07:10:17 UTC
IP Threat Analysis
No Threats Found

Recorded Future


Recorded Future
IP ADDRESS
210.122.9.62
References 8
First Reference May 5, 2022
Latest Reference May 5, 2022
ASN AS9848
ORG Sejong Telecom
GEO South Korea
Recorded Future Community IP Address
Used in List Shodan: CVE-2014-0160 Heartbleed Vulnerable SSL Hosts
5
UNUSUAL
RISK SCORE
1 of 71 Risk Rules Triggered
Show recent events or cyber events
Recorded Future AI Insights
Insufficient Information for Analysis
Recorded Future AI will produce insights when there are 3 or more risk rules triggered.

❖ **SPF, DKIM & DMARC Status (PASS/FAIL)**

SPF-None

DKIM-None

DMARC-Skipped

❖ **Content Analysis**

URL Analysis

1) https[:]//aquapham[.]net/viewer/?ur=email&dn=domain[.]com

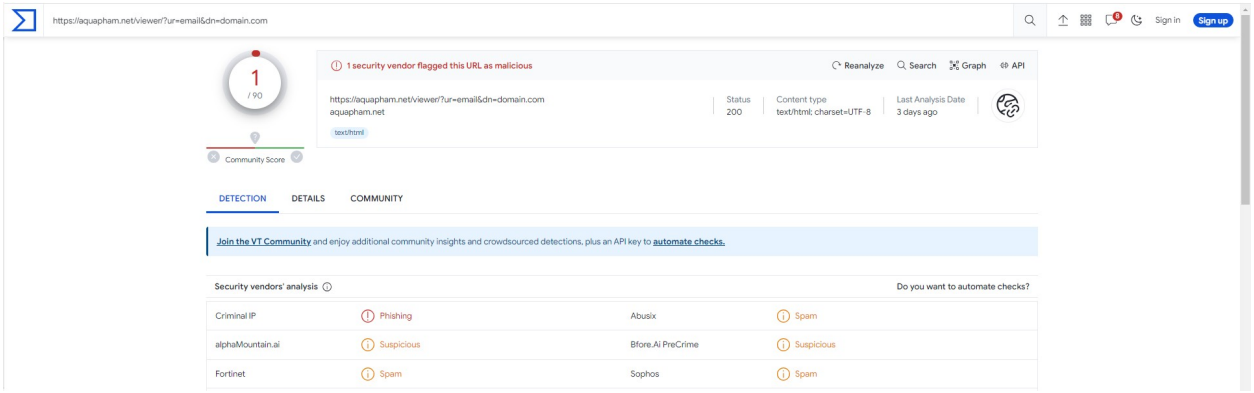
Reputation-**Phishing**

URL Hosted IP- 45[.]141[.]152[.]19

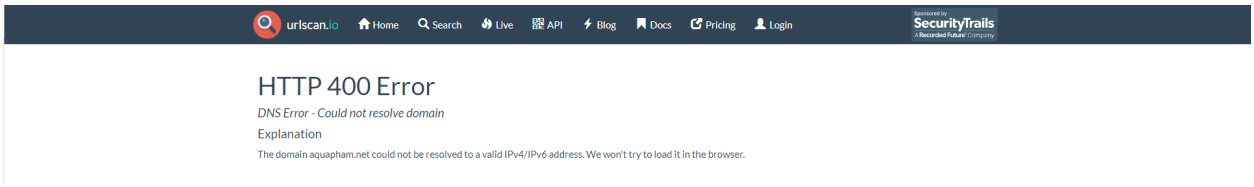
Verdict**-Malicious**

(VT-3,RF-33,IPVoid-4,AbuseIPDB-61%,BrightCloud-High Risk for Phishing)

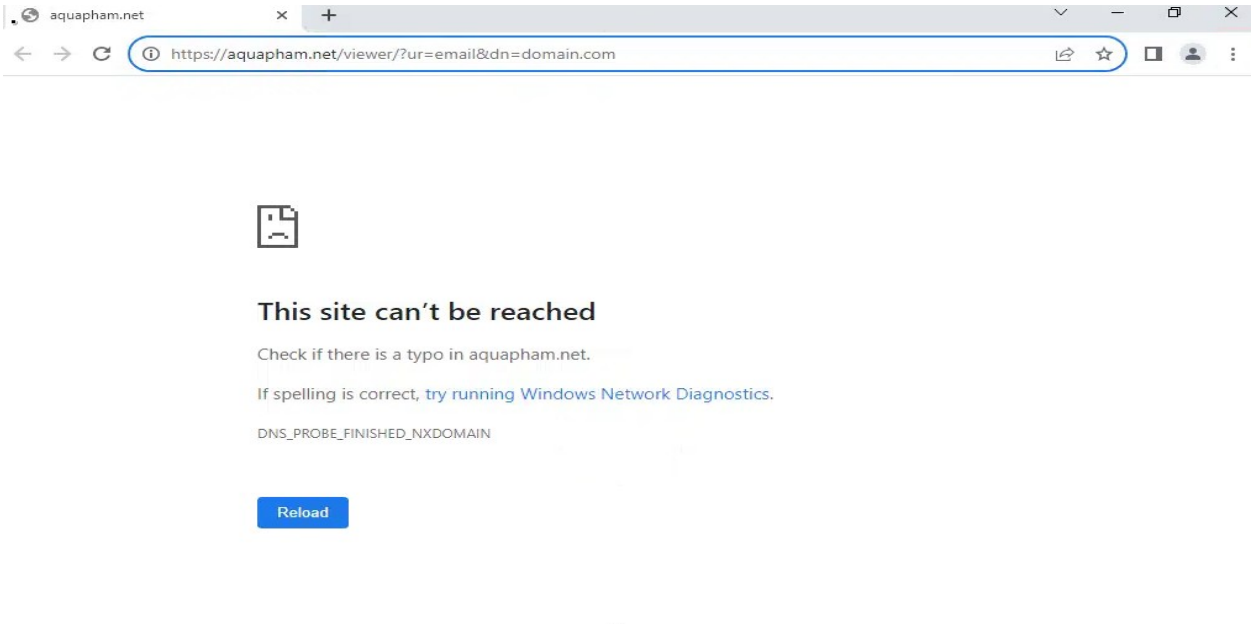
Virus Total



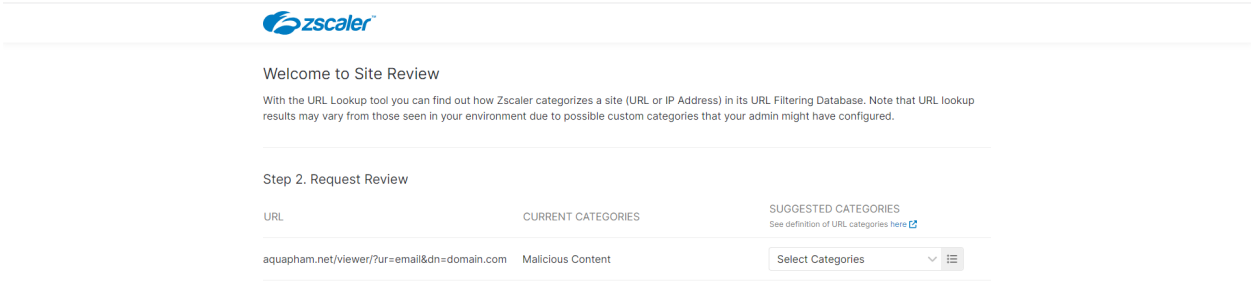
URLScanIO



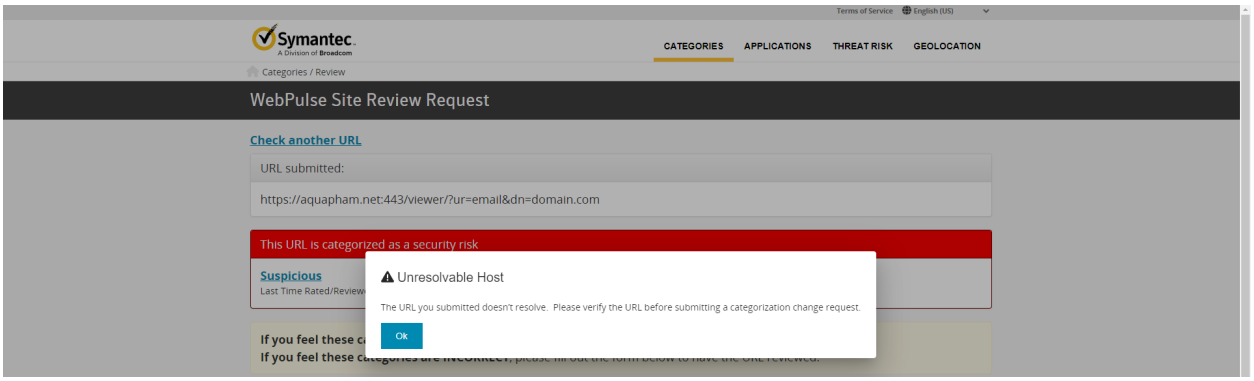
Browserling

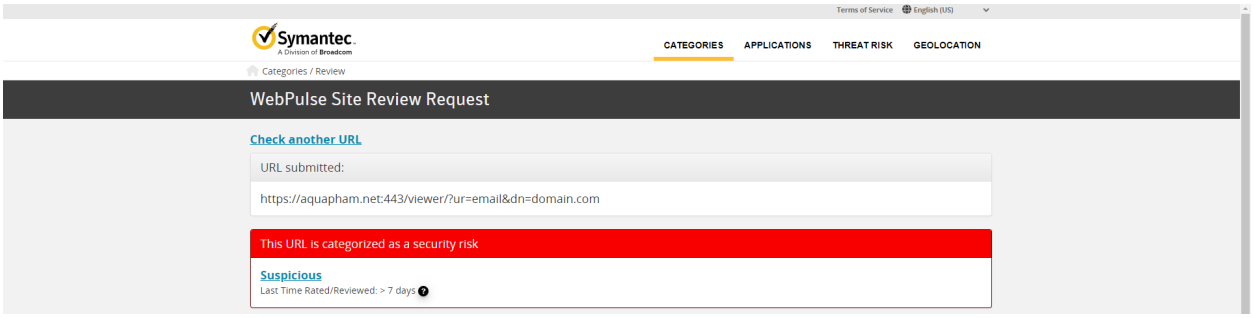


Zscaler Site Review

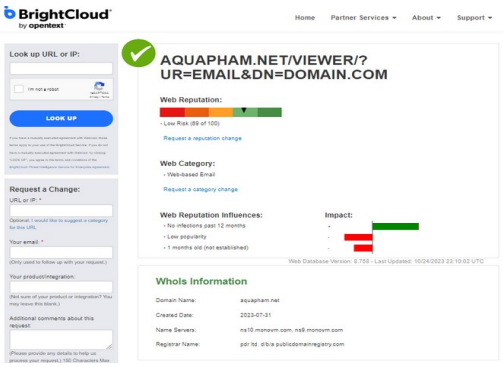

zscaler
Welcome to Site Review
With the URL Lookup tool you can find out how Zscaler categorizes a site (URL or IP Address) in its URL Filtering Database. Note that URL lookup results may vary from those seen in your environment due to possible custom categories that your admin might have configured.
Step 2. Request Review
URL
CURRENT CATEGORIES
SUGGESTED CATEGORIES
See definition of URL categories here
aquapham.net/viewer/?ur=email&dn=domain.com
Malicious Content
Select Categories

Symantec Site Review





BrightCloud



2) https[:]//protect.docusign.net/report-abuse?e=AUtomjpFak9GlbPL0zFFi11rxo2a-L1l0xL9xVFfCnMLPrRH-kEUxclfSilx1Rl9NoYynu2kl0PLTneyDgqvPh2kaLzX2GWMcrpnKa_WguA7j8YnLTm4mV3py6FKwyJw5neKuzTo2DTmkzV6c9_OH8-xZi62l_lAuyQRZUj6x-2EUuVAty5_wXCFE8HsIBnfETBp9I2jU-GWJrZLVQuN6Jgq0SPcPPIRPYAfuIMuS4xv_NNkOqZrjFo4WztXYDHz6BPCs2Vz4--Y3QsgJdRSpXeg7EL20XeC2PMks8JcSXjTthFEtZFlT-FJNUx8OwI5L7KbE2D4WmVvRkREz03STmh5RfAJFNTwP8XcZj8snRw_uQ7OEb_0JSg_wf8989LmbrrxVFLdVGaDaU_xnjkh65hXWaXxp6FfMWRphCrm18NFL5UqPYTV3q2pbw8-lFnjeX3O9SAUwoGSp0OJwJ9zf0B5FMLYGUCUsuDoCsr5ko_6&lang=en

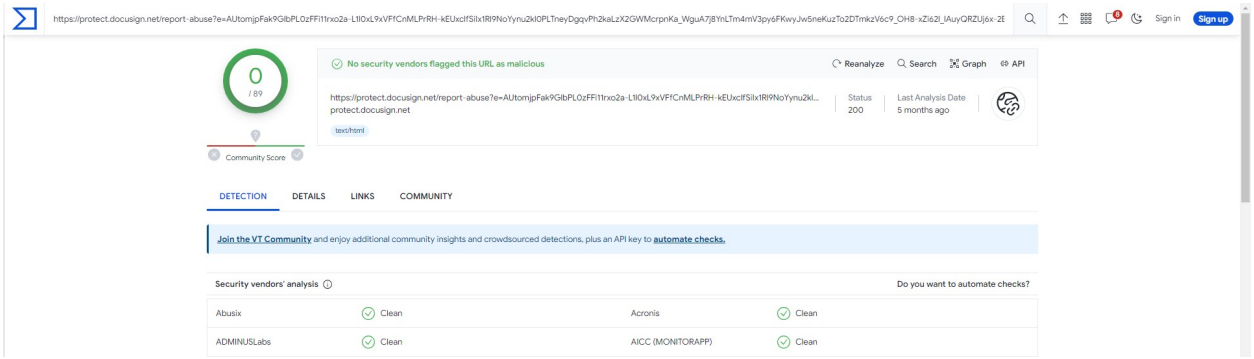
Reputation-**Clean**

URL Hosted IP- 64[.]207[.]218[.]159

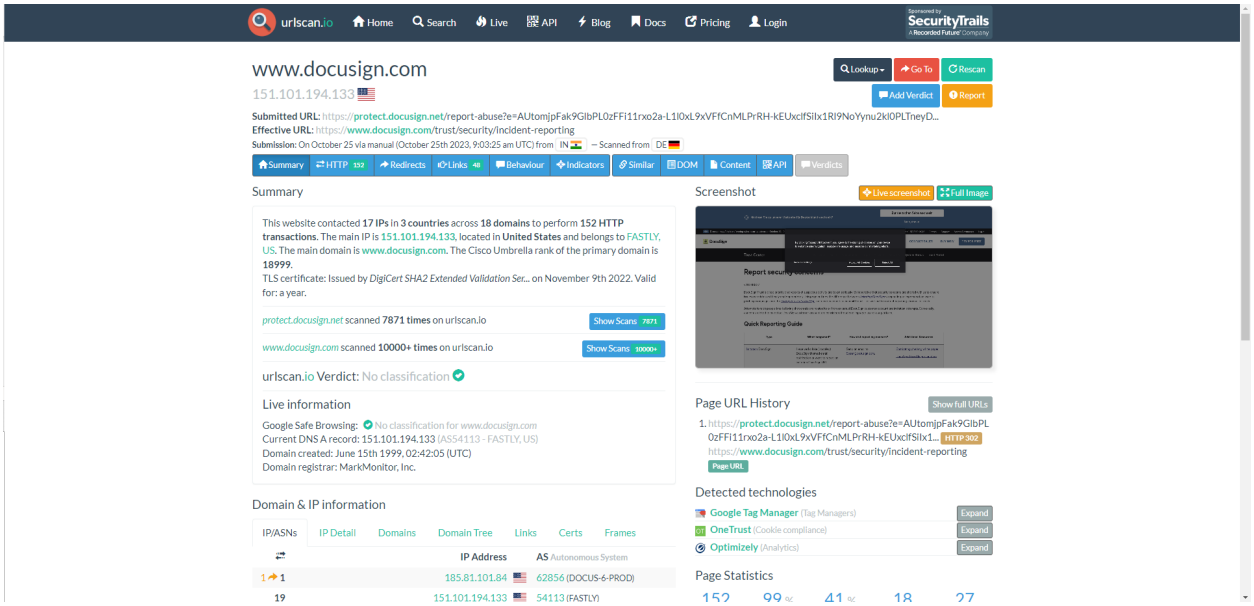
Verdict**-Clean**

(VT-0,RF-0,IPVoid-0,AbuseIPDB-0%,BrightCloud-Benign)

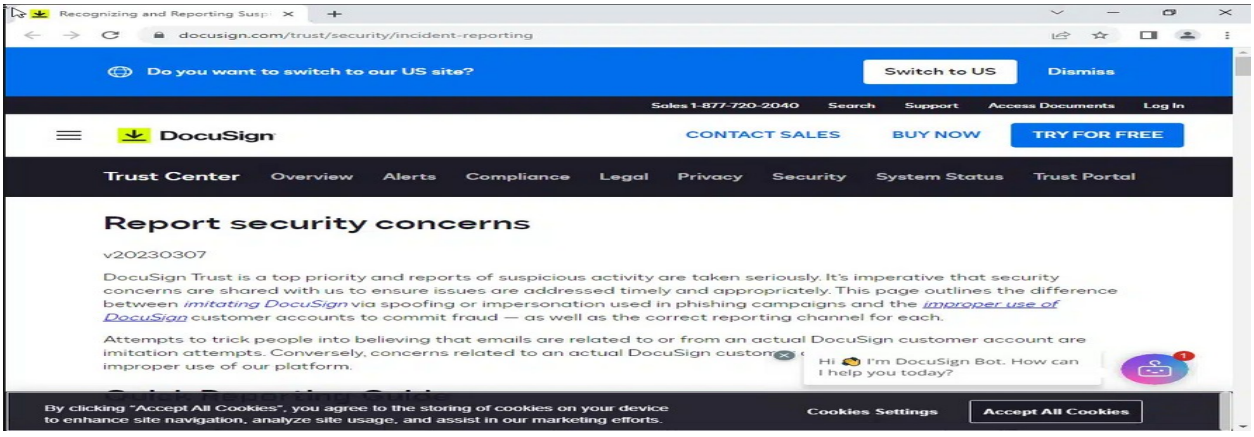
Virus Total



URLScanIO

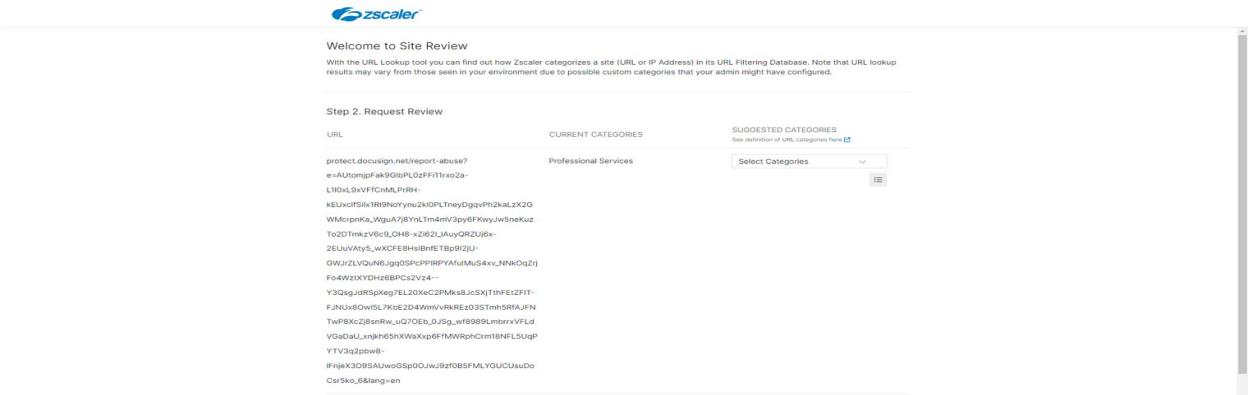


Browserling

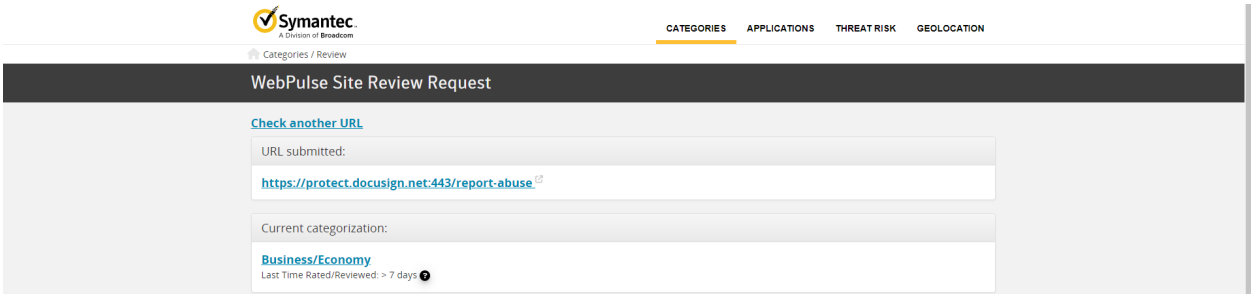


TCS Confidential

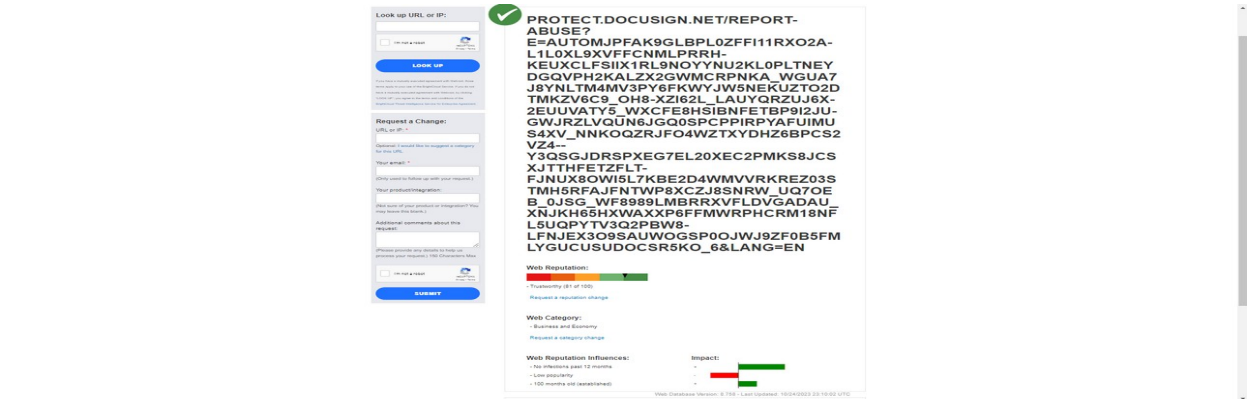
Zscaler Site Review


zscaler
Welcome to Site Review
With the URL Lookup tool you can find out how Zscaler categorizes a site (URL or IP Address) in its URL Filtering Database. Note that URL lookup results may vary from those seen in your environment due to possible custom categories that your admin might have configured.
Step 2. Request Review
URL
CURRENT CATEGORIES
SUGGESTED CATEGORIES
See definition of URL categories here
protect.docusign.net/report-abuse?e=AUtomjpFak9GlbPL0zFFI11rxo2a-L1l0xL9xVFfCnMLPrRH-kEUxclfSIlx1Rl9NoYynu2kl0PLTneyDgqvPh2kaLzX2GWMcrpnKa_WguA7j8YnLTm4mV3py6FKwyJw5neKuzTo2DTmkzV6c9_OH8-xZi62l_lAuyQRZUj6x-2EUuVAty5_wXCFE8HsIBnfETBp9I2jU-GWJrZLVQuN6JgqOSPcPPIRPYAfulMuS4xv_NNkOqZrjFo4WztXYDHz6BPCs2Vz4--Y3QsgJdRSpXeg7EL20XeC2PMks8JcSXjTthFEtZFIT-FJNUx8Owl5L7KbE2D4WmVvRkREz03STmh5RfAJFNTwP8XcZj8snRw_uQ7OEb_0JSg_wf8989LmbrrxVFLdVGaDaU_xnjkh65hXWaXxp6FfMWRphCrmt8NFL5UqPYTV3q2pbw8-IFnjeX3O9SAUwoGSp0OJwJ9zf0B5FMLYGUCUsuDoCsr5ko_6&lang=en
Professional Services
Select Categories

Symantec Site Review



BrightCloud



3) https[:]//support.docusign.com/en/guides/Declining-to-sign-DocuSign-Signer-Guide

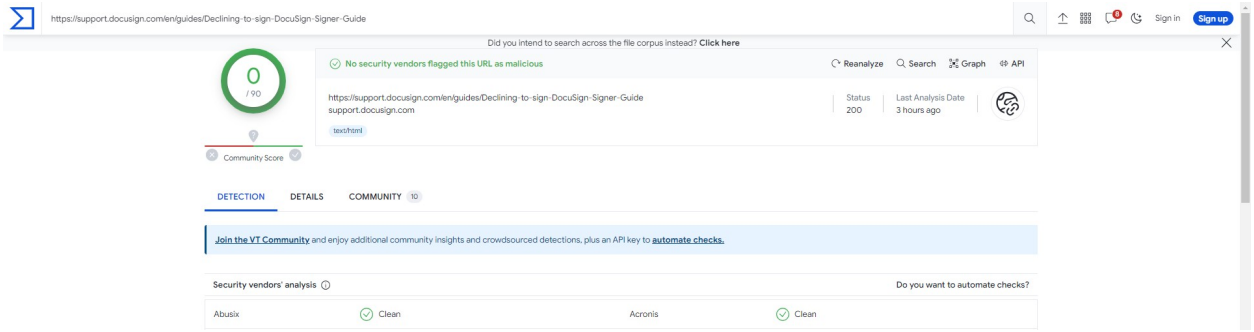
Reputation**-Clean**

URL Hosted IP- 13[.]110[.]26[.]11

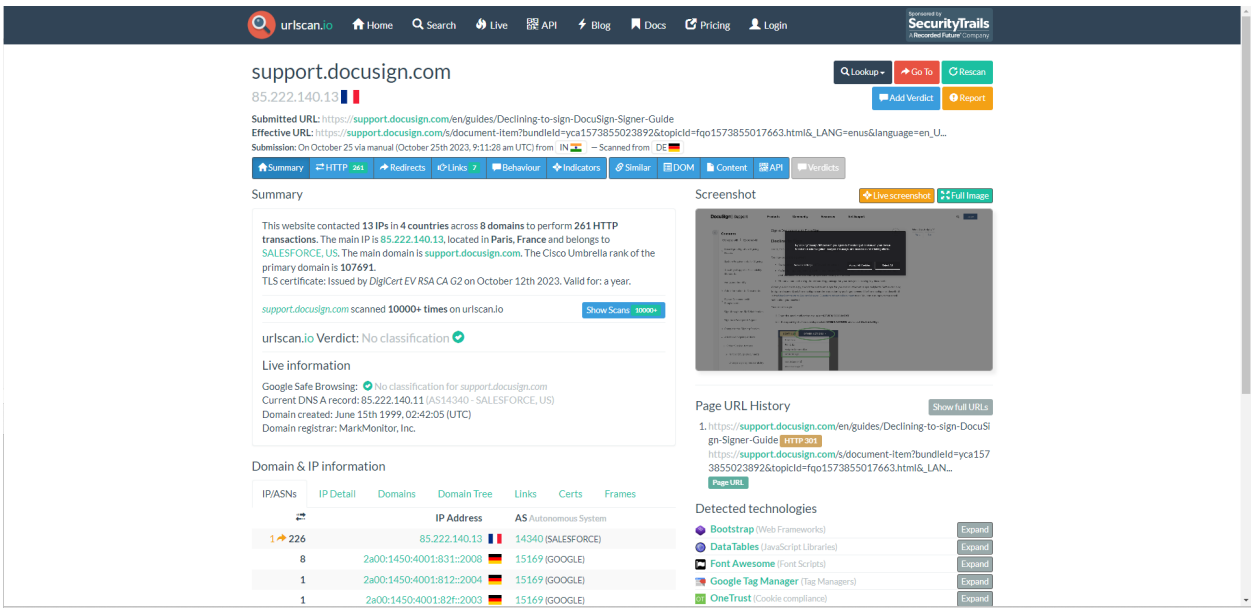
Verdict**-Clean**

(VT-0,RF-0,IPVoid-0,AbuseIPDB-0%,BrightCloud-Benign)

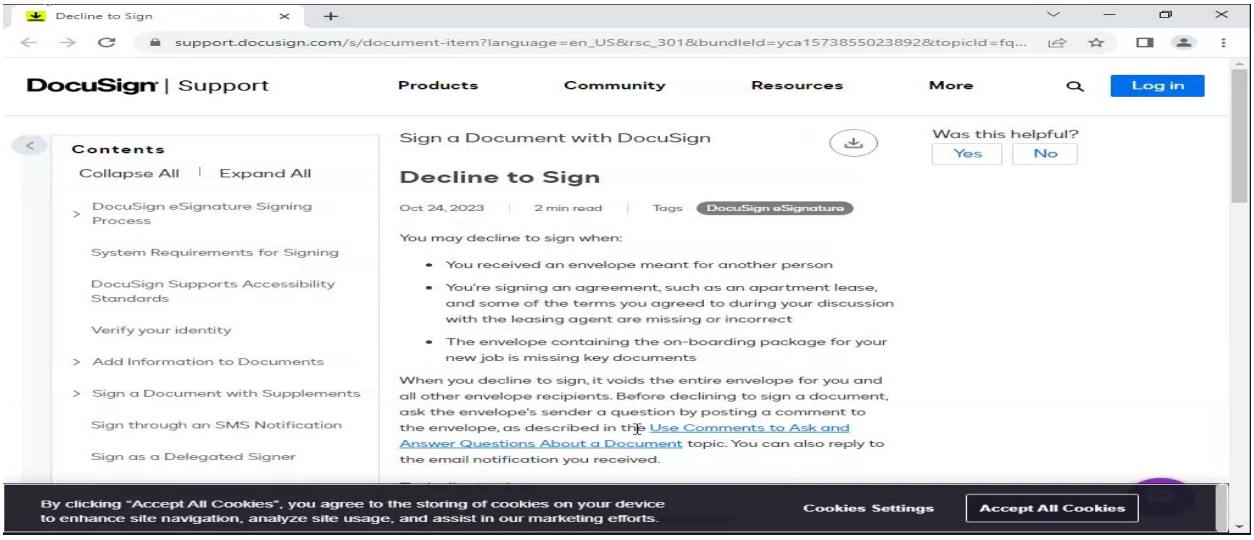
Virus Total



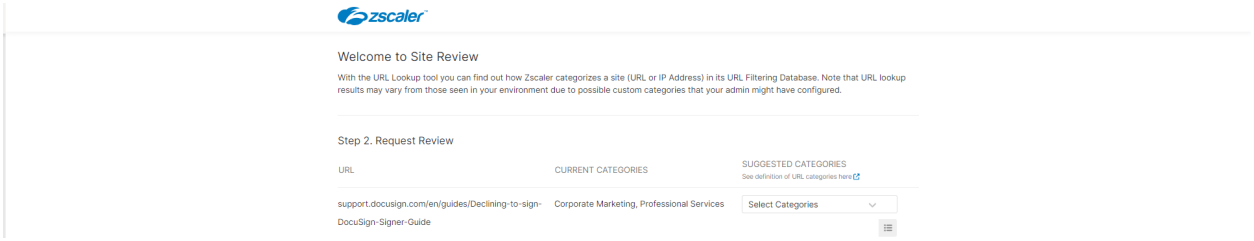
URLScanIO



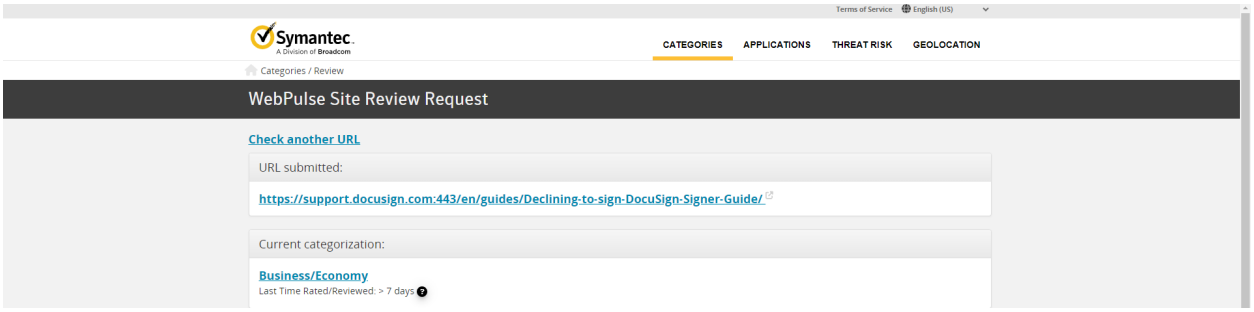
Browserling


Decline to Sign
support.docusign.com/s/document-item?language=en_US&rsc_301&bundleId=yca1573855023892&topicId=fq...
DocuSign | Support
Products
Community
Resources
More
Log in
Contents
Collapse All | Expand All
DocuSign eSignature Signing Process
System Requirements for Signing
DocuSign Supports Accessibility Standards
Verify your identity
Add Information to Documents
Sign a Document with Supplements
Sign through an SMS Notification
Sign as a Delegated Signer
Sign a Document with DocuSign
Decline to Sign
Oct 24, 2023 | 2 min read | Tags DocuSign eSignature
You may decline to sign when:
You received an envelope meant for another person
You're signing an agreement, such as an apartment lease, and some of the terms you agreed to during your discussion with the leasing agent are missing or incorrect
The envelope containing the on-boarding package for your new job is missing key documents
When you decline to sign, it voids the entire envelope for you and all other envelope recipients. Before declining to sign a document, ask the envelope's sender a question by posting a comment to the envelope, as described in the Use Comments to Ask and Answer Questions About a Document topic. You can also reply to the email notification you received.
Was this helpful?
Yes
No
By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts.
Cookies Settings
Accept All Cookies

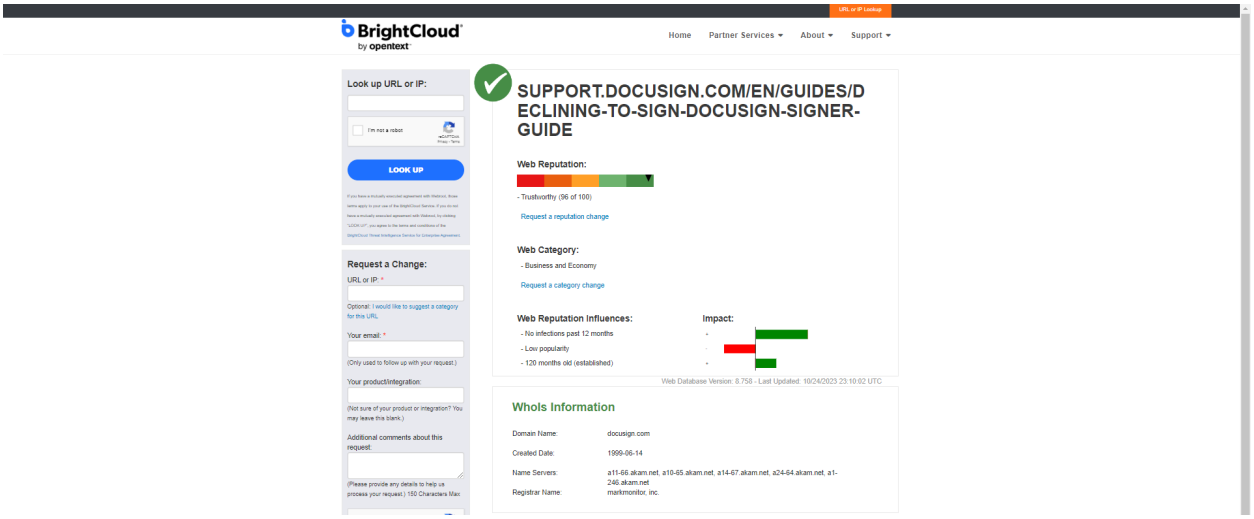
Zscaler Site Review


zscaler
Welcome to Site Review
With the URL Lookup tool you can find out how Zscaler categorizes a site (URL or IP Address) in its URL Filtering Database. Note that URL lookup results may vary from those seen in your environment due to possible custom categories that your admin might have configured.
Step 2. Request Review
URL
CURRENT CATEGORIES
SUGGESTED CATEGORIES
See definition of URL categories here
support.docusign.com/en/guides/Declining-to-sign-DocuSign-Signer-Guide
Corporate Marketing, Professional Services
Select Categories

Symantec Site Review



BrightCloud



4) https[:]//support.docusign.com/en/articles/How-do-I-manage-my-email-notifications

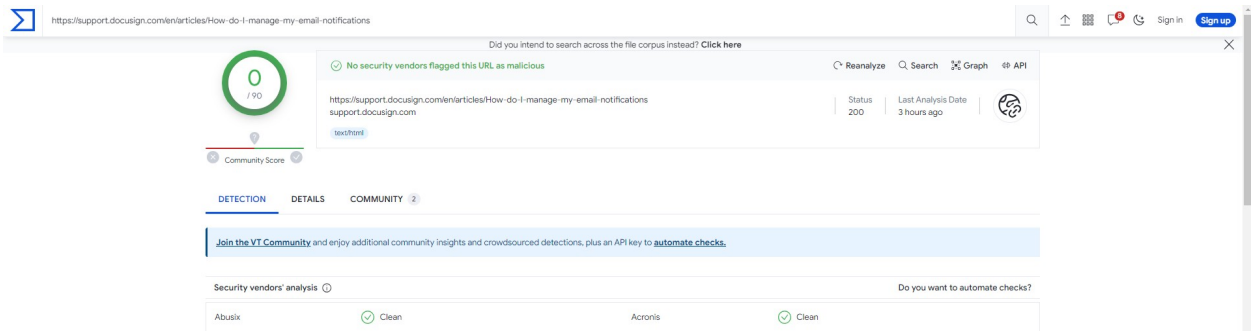
Reputation-**Clean**

URL Hosted IP- 13[.]110[.]26[.]13

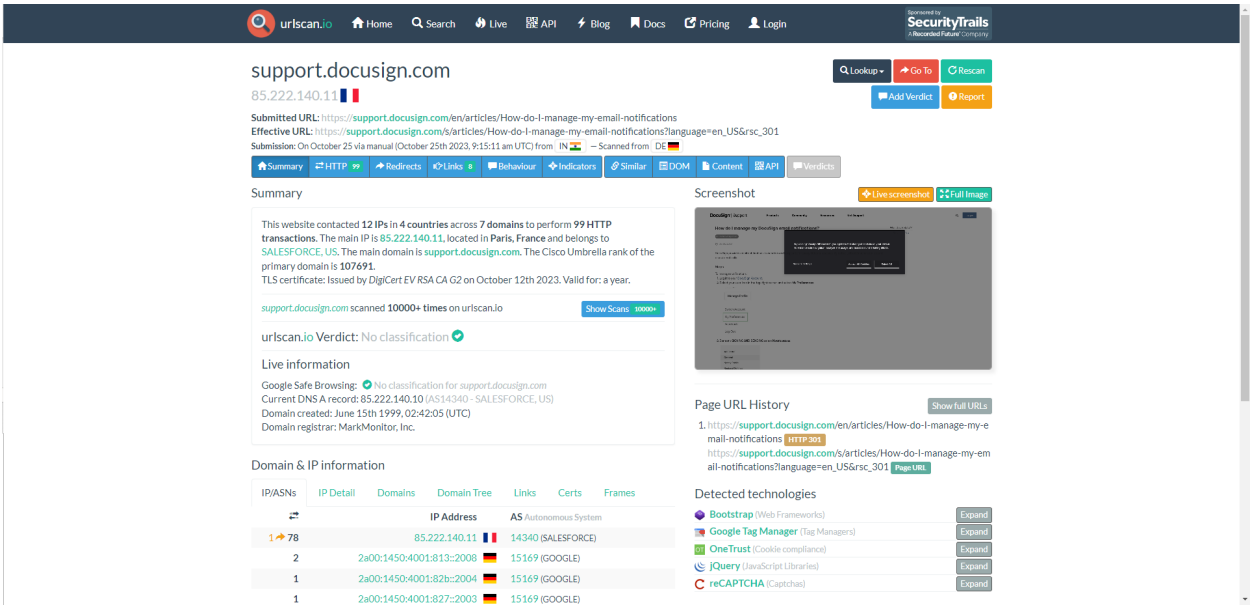
Verdict**-Clean**

(VT-0,RF-0,IPVoid-0,AbuseIPDB-0%,BrightCloud-Benign)

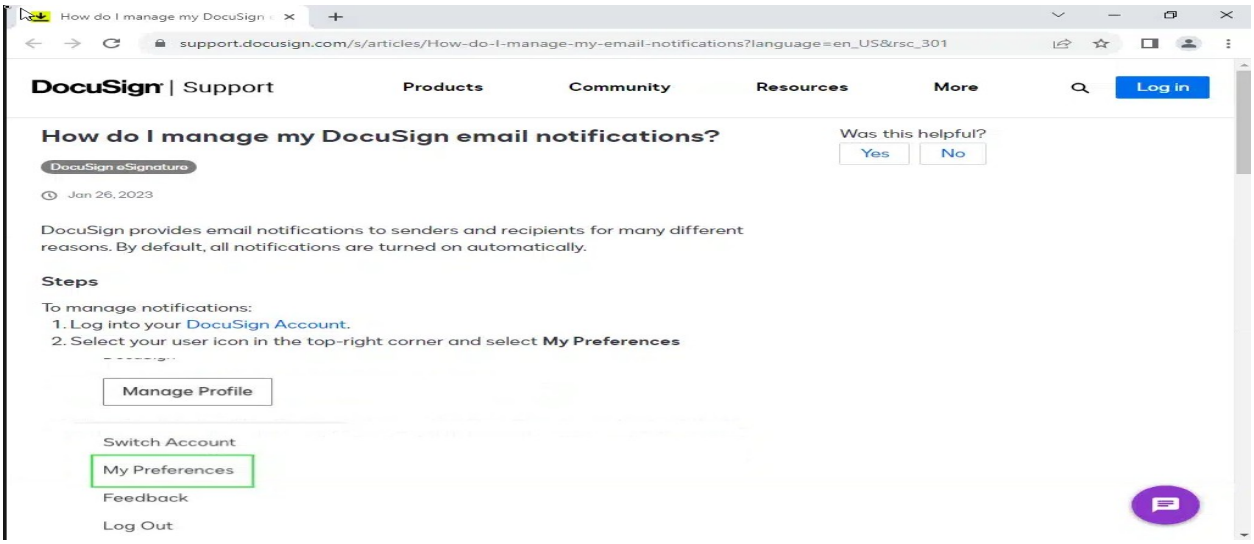
Virus Total



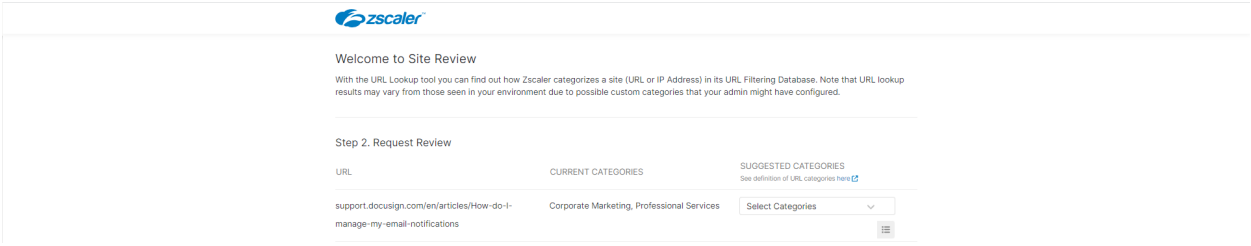
URLScanIO



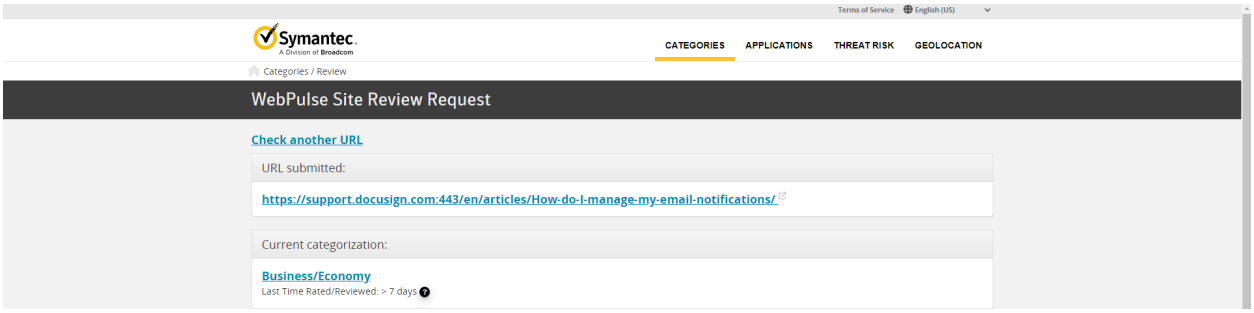
Browserling



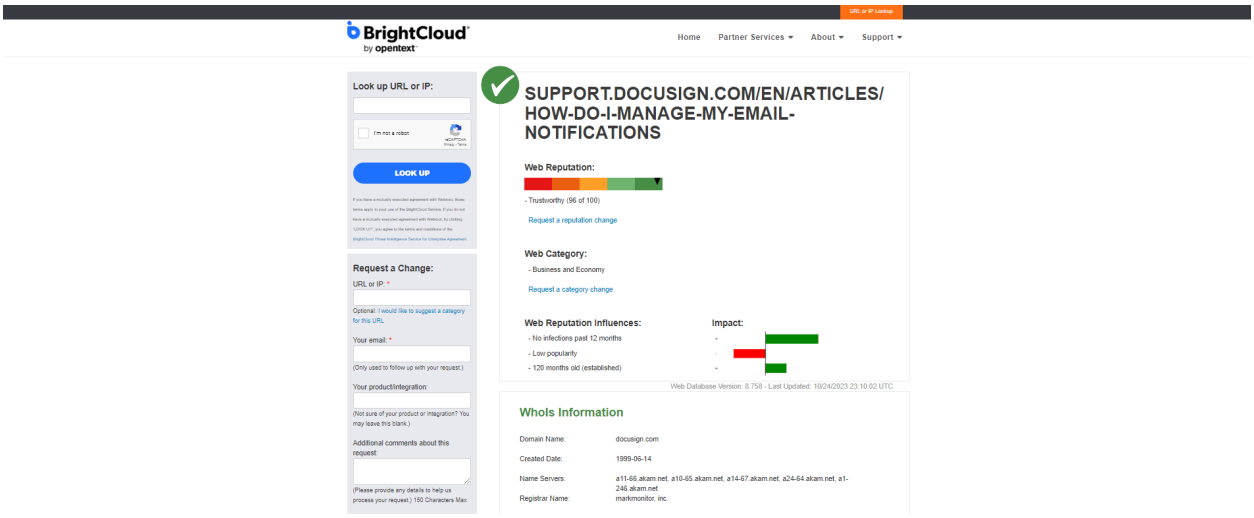
Zscaler Site Review


zscaler
Welcome to Site Review
With the URL Lookup tool you can find out how Zscaler categorizes a site (URL or IP Address) in its URL Filtering Database. Note that URL lookup results may vary from those seen in your environment due to possible custom categories that your admin might have configured.
Step 2. Request Review
URL
CURRENT CATEGORIES
SUGGESTED CATEGORIES
See definition of URL categories here
support.docusign.com/en/articles/How-do-I-manage-my-email-notifications
Corporate Marketing, Professional Services
Select Categories

Symantec Site Review



BrightCloud


BrightCloud
by opentext
Home
Partner Services
About
Support
Look up URL or IP:
I'm not a robot
LOOK UP
Request a Change:
URL or IP: *
Optional: I would like to suggest a category for this URL.
Your email: *
(Only used to follow up with your request.)
Your product/integration:
(Not sure of your product or integration? You may leave this blank.)
Additional comments about this request:
(Please provide any details to help us process your request.) 150 Characters Max.
SUPPORT.DOCUSIGN.COM/EN/ARTICLES/HOW-DO-I-MANAGE-MY-EMAIL-NOTIFICATIONS
Web Reputation:
- Trustworthy (96 of 100)
Request a reputation change
Web Category:
- Business and Economy
Request a category change
Web Reputation Influences:
- No infections past 12 months
- Low popularity
- 120 months old (established)
Impact:
Web Database Version: 8.758 - Last Updated: 10/24/2023 23:10:02 UTC
Whois Information
Domain Name: docusign.com
Created Date: 1999-06-14
Name Servers: a11-66.akam.net, a10-65.akam.net, a14-67.akam.net, a24-64.akam.net, a1-246.akam.net
Registrar Name: markmonitor, inc.

5) https[:]//www.docusign.com/support

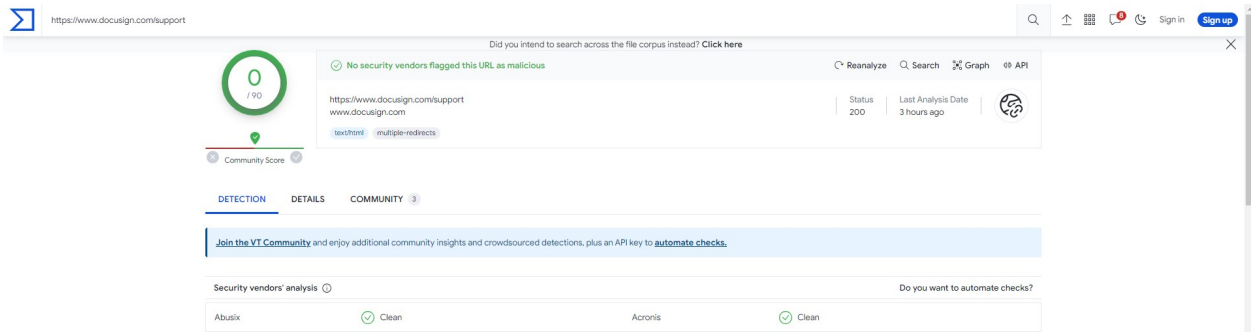
Reputation**-Clean**

URL Hosted IP- 151[.]101[.]194[.]133

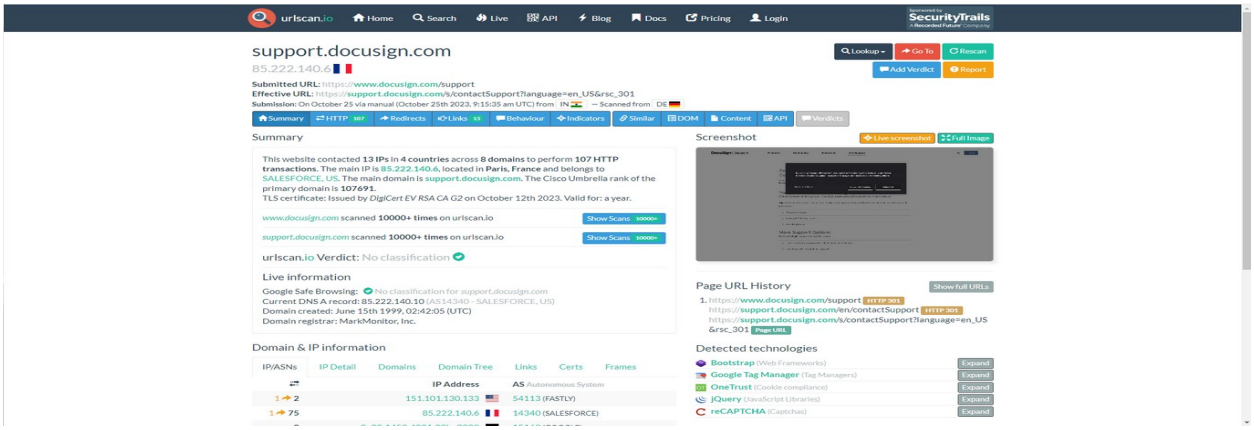
Verdict**-Suspicious**

(VT-0,RF-35,IPVoid-1,AbuseIPDB-Whitelisted,BrightCloud-High Risk for Phishing & Proxy)

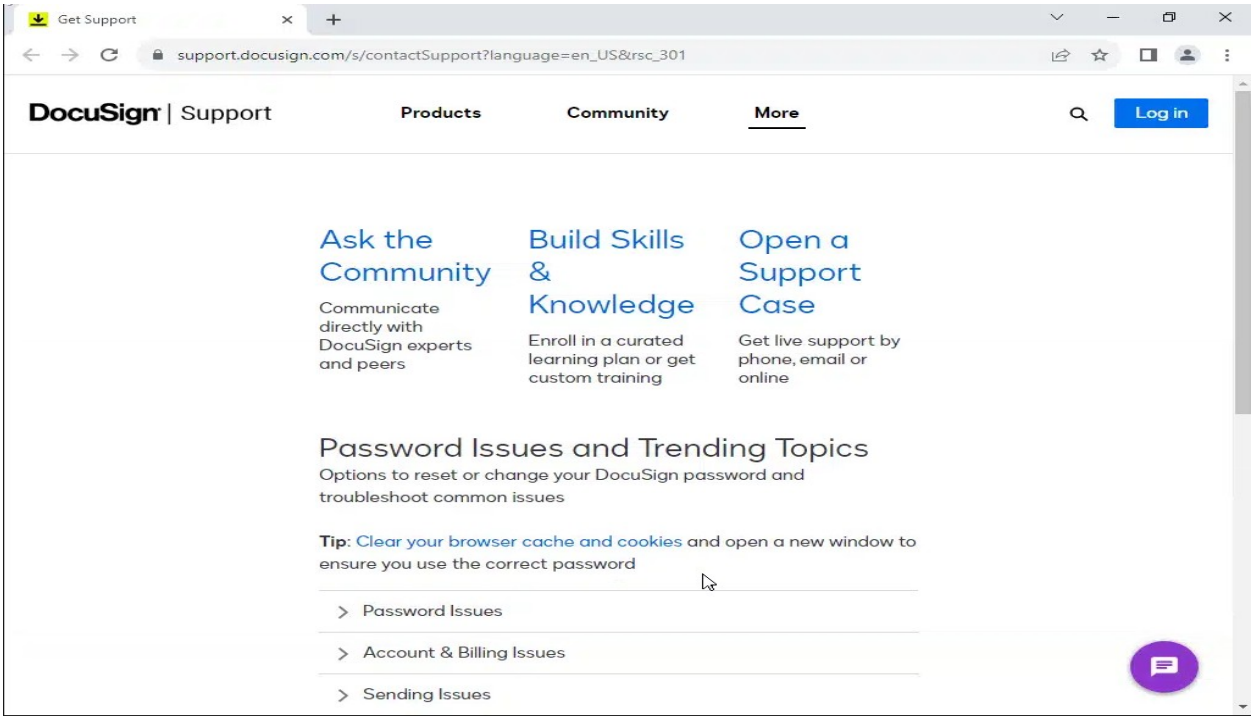
Virus Total



URLScanIO

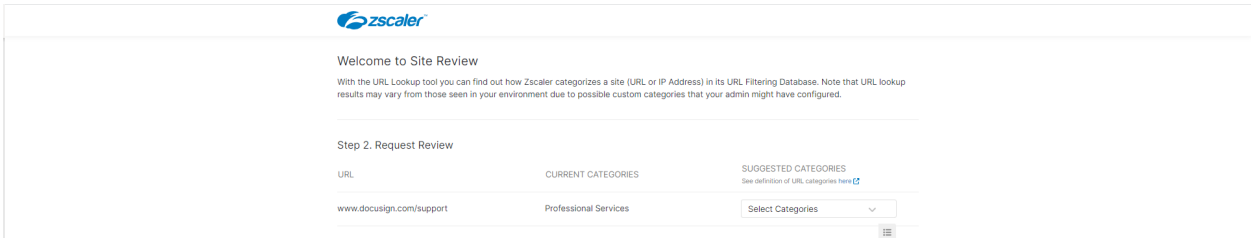


Browserling

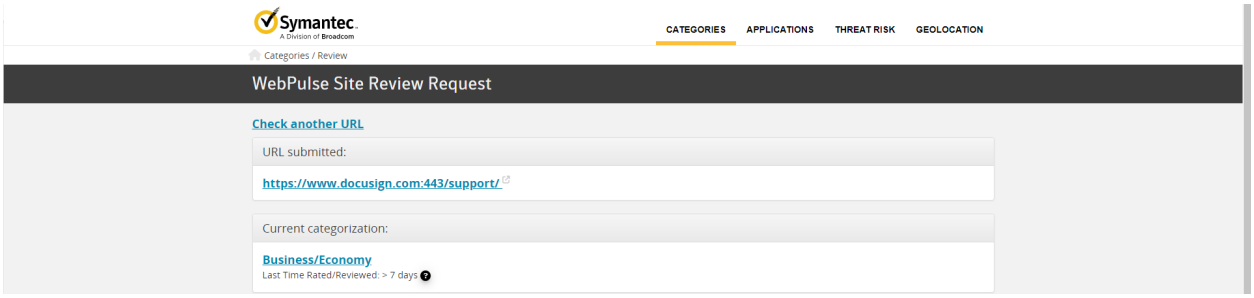

Get Support
support.docusign.com/s/contactSupport?language=en_US&rsc_301
DocuSign | Support
Products
Community
More
Log in
Ask the Community
Communicate directly with DocuSign experts and peers
Build Skills & Knowledge
Enroll in a curated learning plan or get custom training
Open a Support Case
Get live support by phone, email or online
Password Issues and Trending Topics
Options to reset or change your DocuSign password and troubleshoot common issues
Tip: Clear your browser cache and cookies and open a new window to ensure you use the correct password
Password Issues
Account & Billing Issues
Sending Issues

Zscaler Site Review

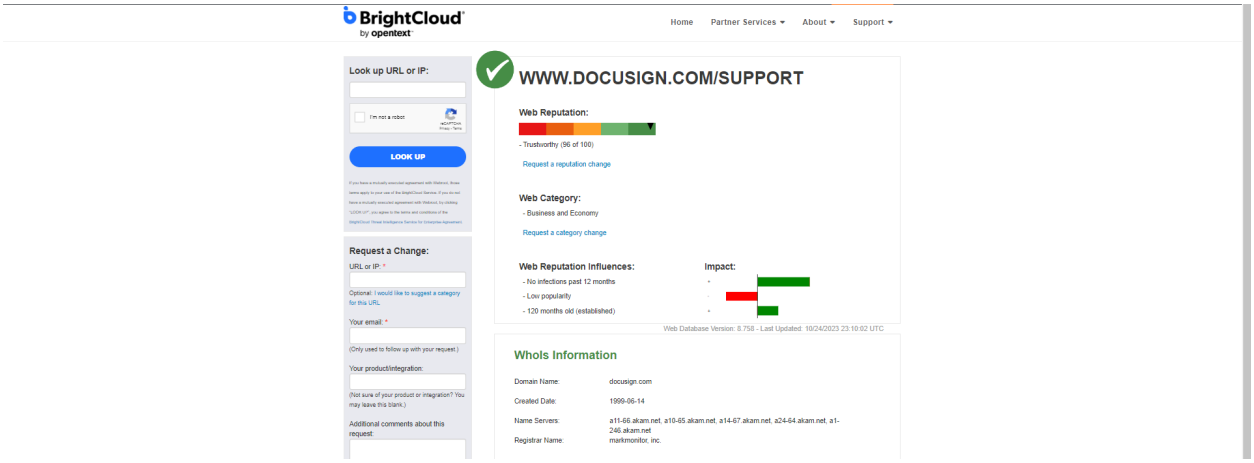
TCS Confidential


zscaler
Welcome to Site Review
With the URL Lookup tool you can find out how Zscaler categorizes a site (URL or IP Address) in its URL Filtering Database. Note that URL lookup results may vary from those seen in your environment due to possible custom categories that your admin might have configured.
Step 2. Request Review
URL
CURRENT CATEGORIES
SUGGESTED CATEGORIES
www.docusign.com/support
Professional Services
Select Categories

Symantec Site Review



BrightCloud



6) https[:]//support.docusign.com/articles/How-do-I-sign-a-DocuSign-document-Basic-Signing

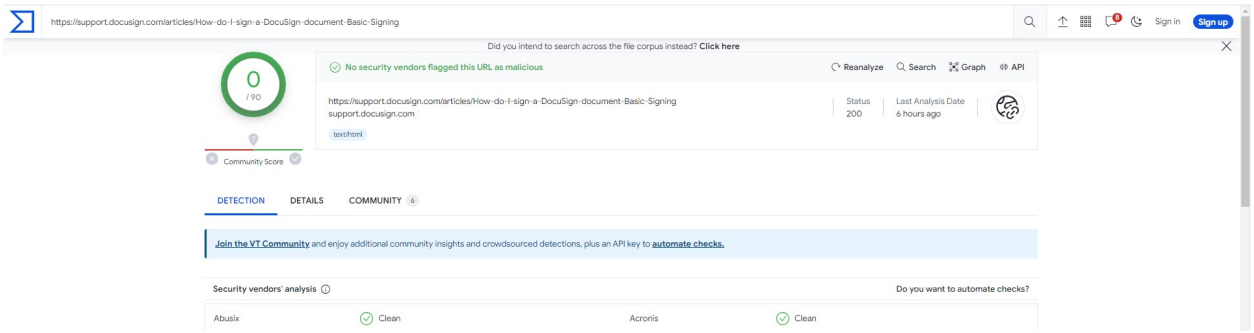
Reputation**-Clean**

URL Hosted IP- 13[.]110[.]26[.]13

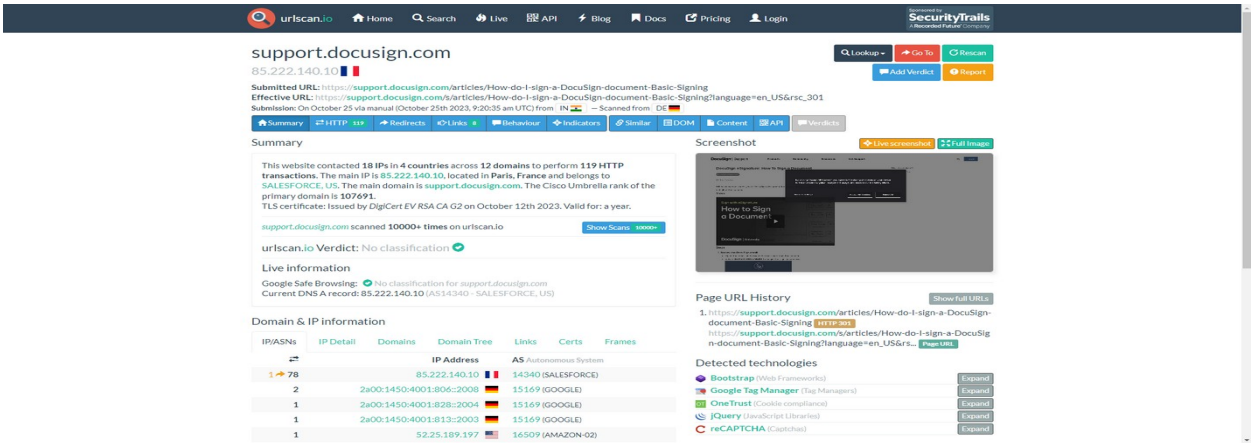
Verdict**-Suspicious**

(VT-0,RF-0,IPVoid-0,AbuseIPDB-0,BrightCloud-Benign)

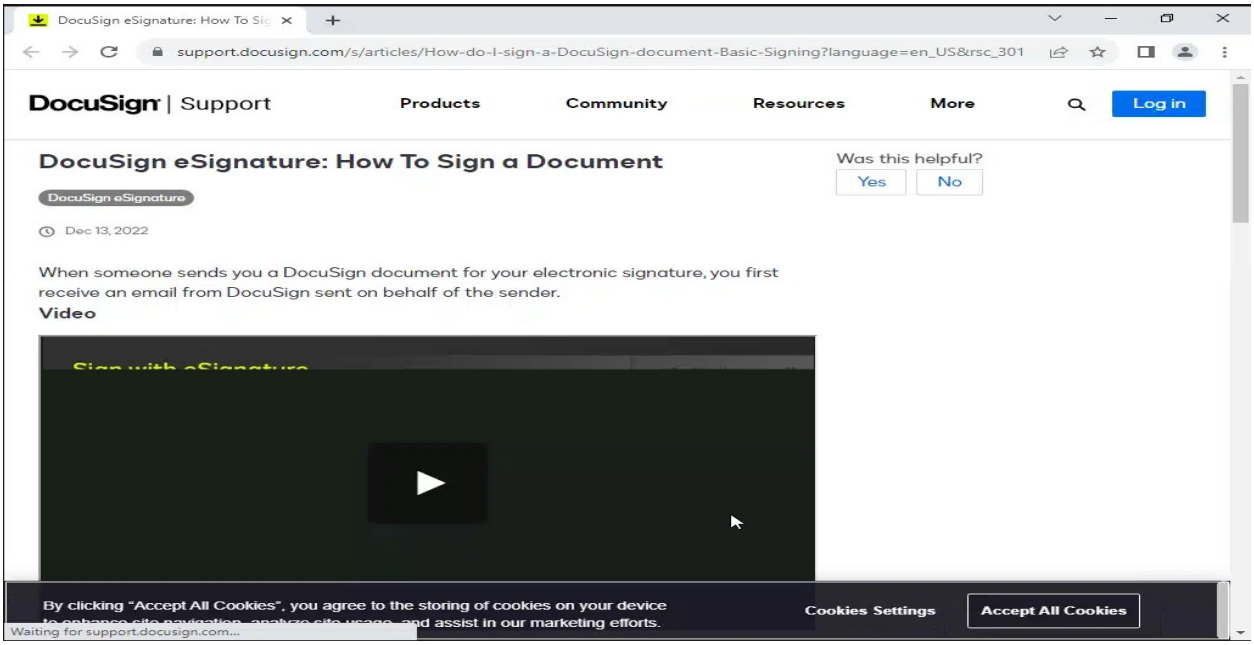
Virus Total



URLScanIO

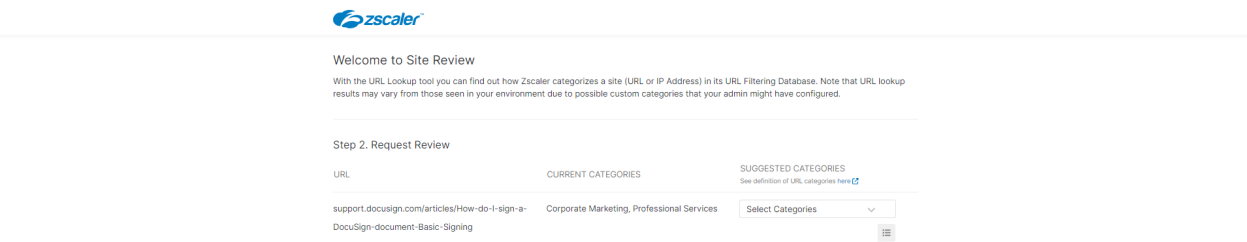


Browserling

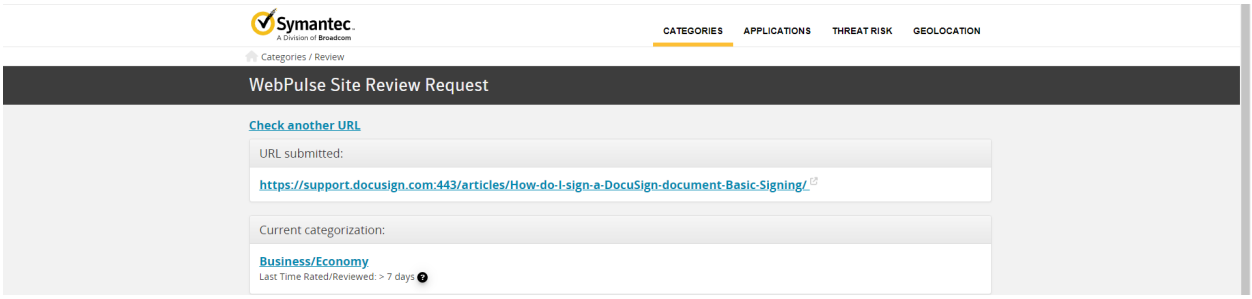

DocuSign eSignature: How To Sig
support.docusign.com/s/articles/How-do-I-sign-a-DocuSign-document-Basic-Signing?language=en_US&rsc_301
DocuSign | Support
Products
Community
Resources
More
Log in
DocuSign eSignature: How To Sign a Document
Was this helpful?
Yes
No
DocuSign eSignature
Dec 13, 2022
When someone sends you a DocuSign document for your electronic signature, you first receive an email from DocuSign sent on behalf of the sender.
Video
By clicking "Accept All Cookies", you agree to the storing of cookies on your device
Cookies Settings
Accept All Cookies
Waiting for support.docusign.com...

Zscaler Site Review

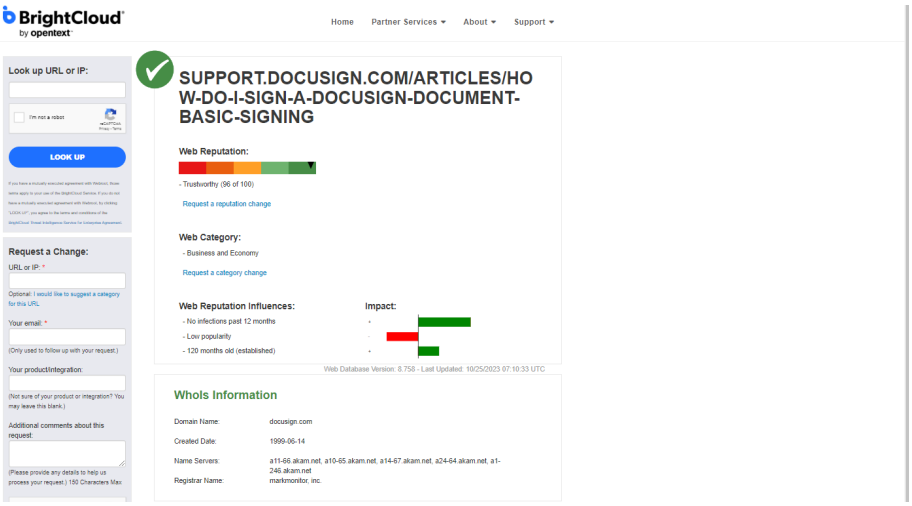
TCS Confidential


zscaler
Welcome to Site Review
With the URL Lookup tool you can find out how Zscaler categorizes a site (URL or IP Address) in its URL Filtering Database. Note that URL lookup results may vary from those seen in your environment due to possible custom categories that your admin might have configured.
Step 2. Request Review
URL
CURRENT CATEGORIES
SUGGESTED CATEGORIES
See definition of URL categories here
support.docusign.com/articles/How-do-I-sign-a-DocuSign-document-Basic-Signing
Corporate Marketing, Professional Services
Select Categories

Symantec Site Review



BrightCloud



7) https[:]//www.docusign.com/features-and-benefits/mobile

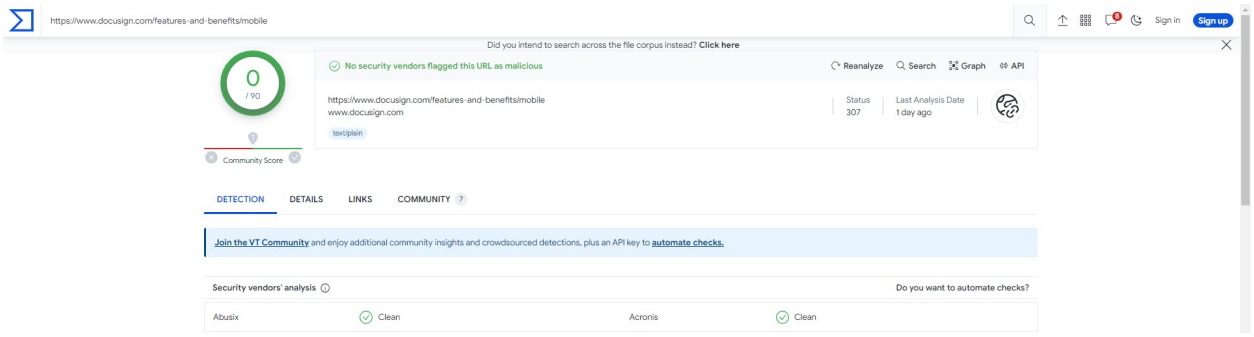
Reputation-Suspicious

URL Hosted IP- 151[.]101[.]130[.]133

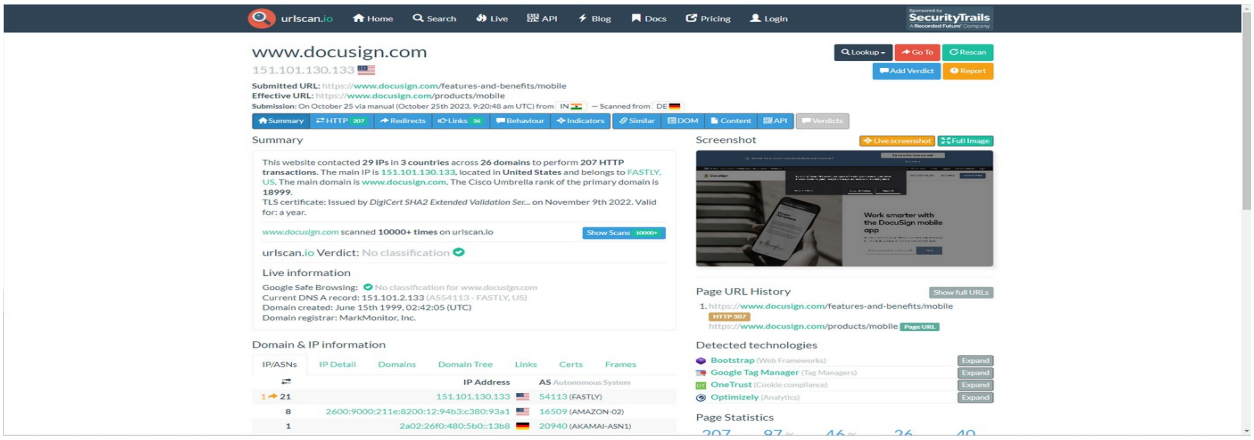
Verdict**-Suspicious**

(VT-0,RF-37,IPVoid-0,AbuseIPDB-Whitelisted,BrightCloud-High Risk for Phishing and Proxy)

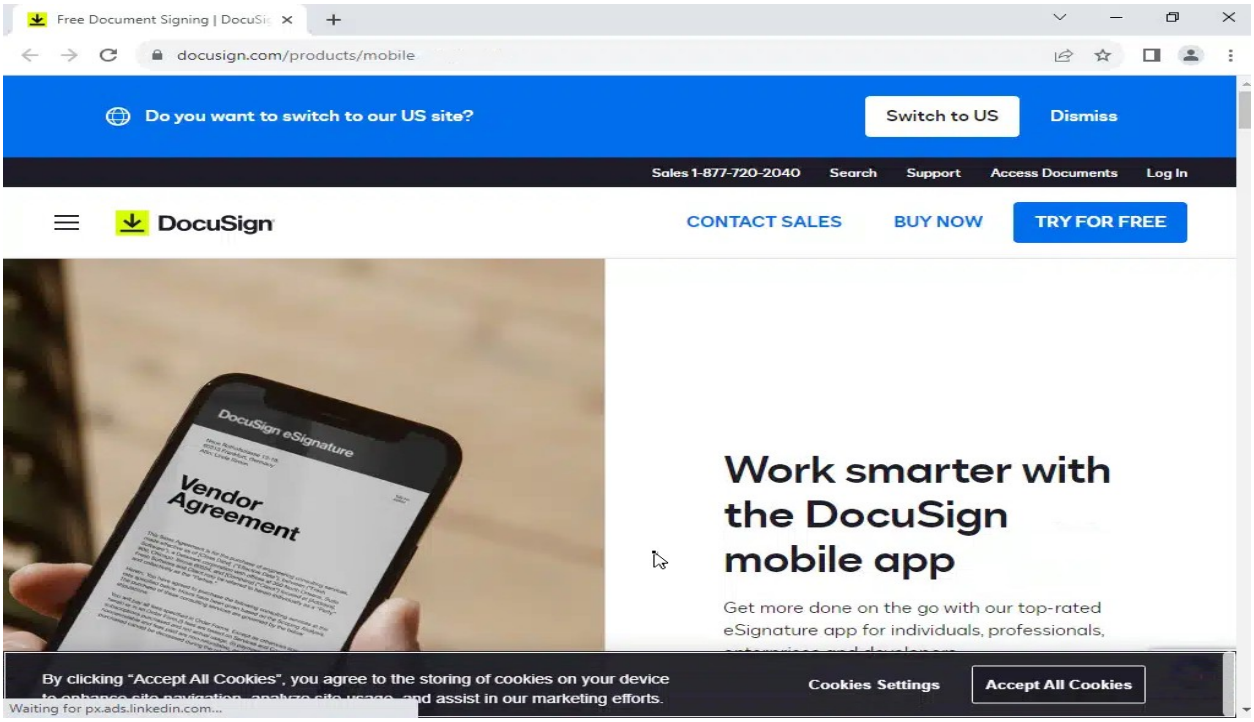
Virus Total



URLScanIO

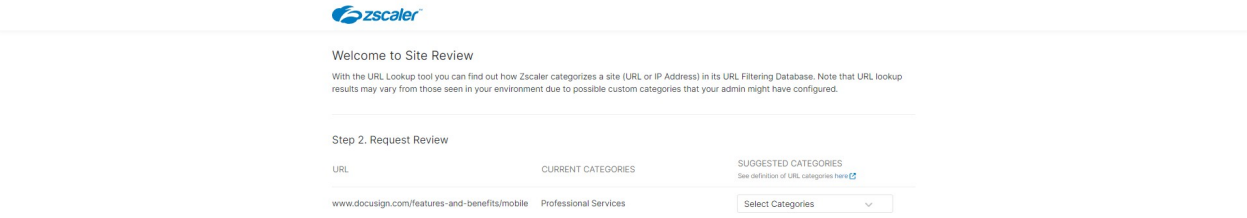


Browserling

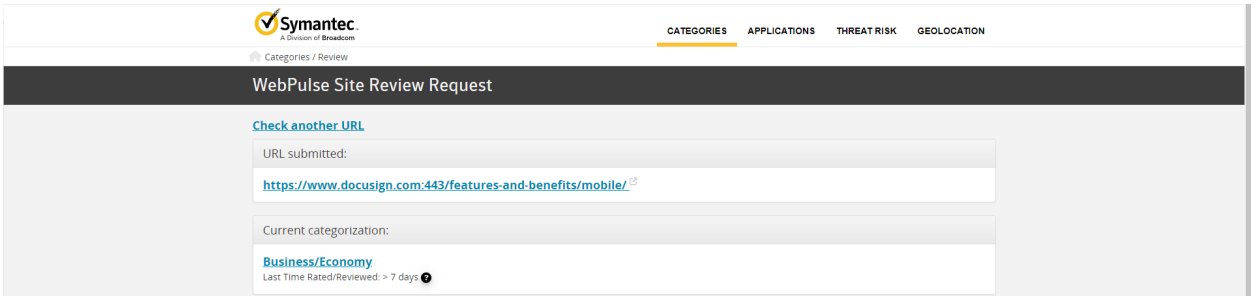

Free Document Signing | DocuSi
docusign.com/products/mobile
Do you want to switch to our US site?
Switch to US
Dismiss
Sales 1-877-720-2040
Search
Support
Access Documents
Log In
DocuSign
CONTACT SALES
BUY NOW
TRY FOR FREE
Work smarter with the DocuSign mobile app
Get more done on the go with our top-rated eSignature app for individuals, professionals,
By clicking "Accept All Cookies", you agree to the storing of cookies on your device
Cookies Settings
Accept All Cookies
Waiting for px.ads.linkedin.com...

Zscaler Site Review

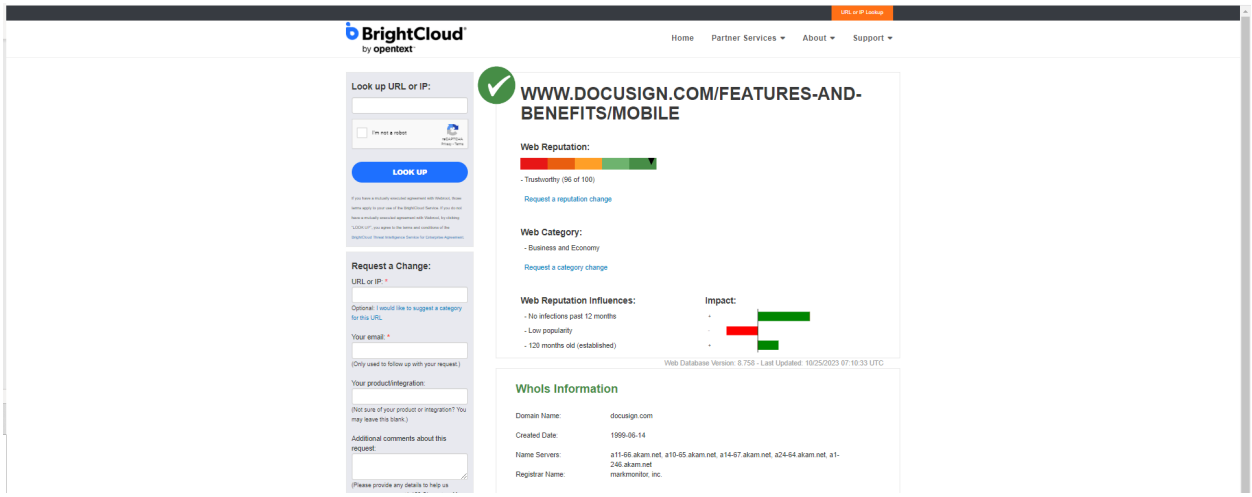
TCS Confidential


zscaler
Welcome to Site Review
With the URL Lookup tool you can find out how Zscaler categorizes a site (URL or IP Address) in its URL Filtering Database. Note that URL lookup results may vary from those seen in your environment due to possible custom categories that your admin might have configured.
Step 2. Request Review
URL
CURRENT CATEGORIES
SUGGESTED CATEGORIES
www.docusign.com/features-and-benefits/mobile
Professional Services
Select Categories

Symantec Site Review

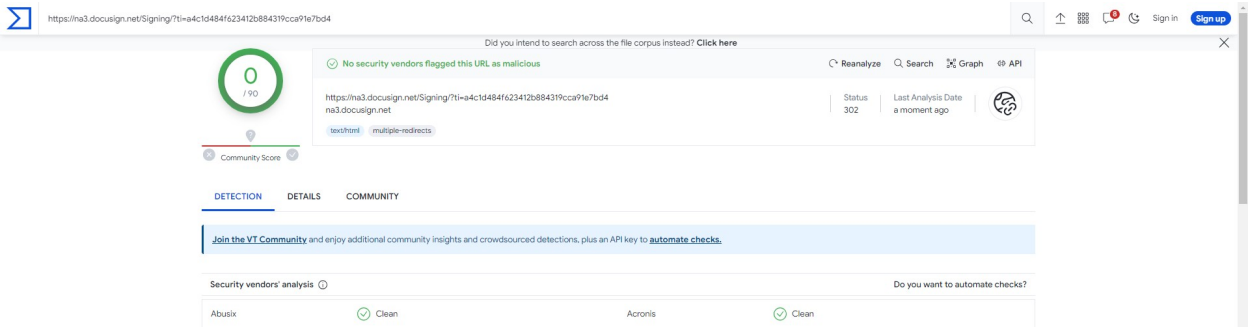


BrightCloud



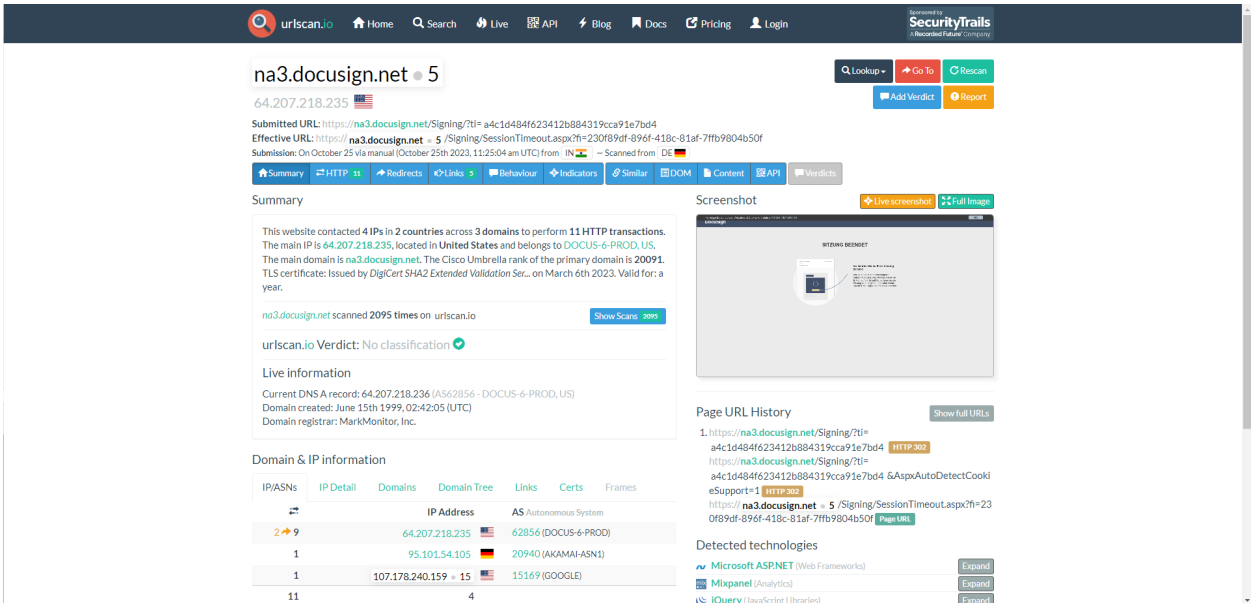
8) https[:]//na3.docusign.net/Signing/?ti=a4c1d484f623412b884319cca91e7bd4

Virus Total

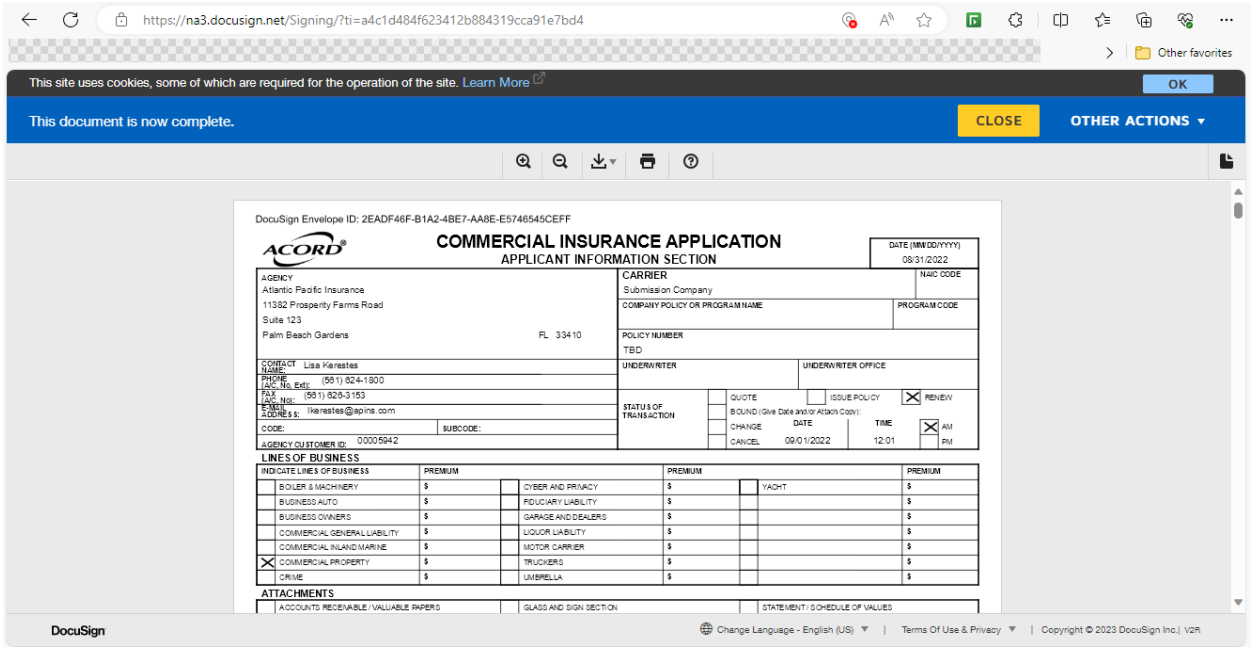


URLScanIO

TCS Confidential

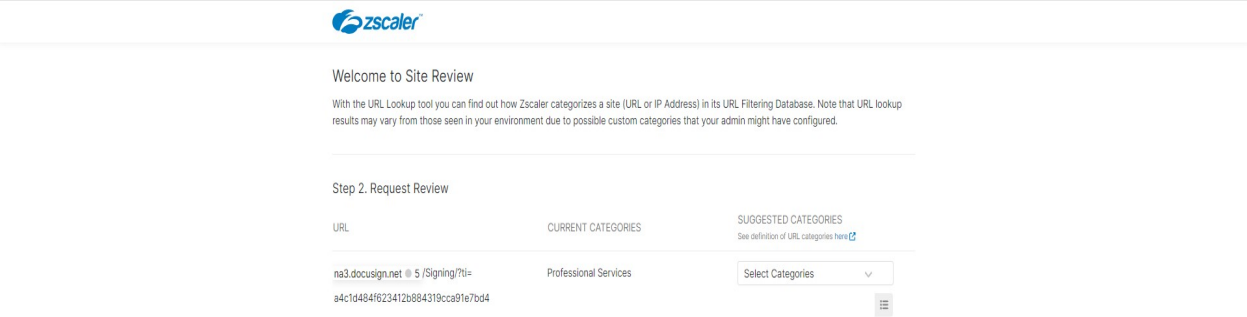


Browserling

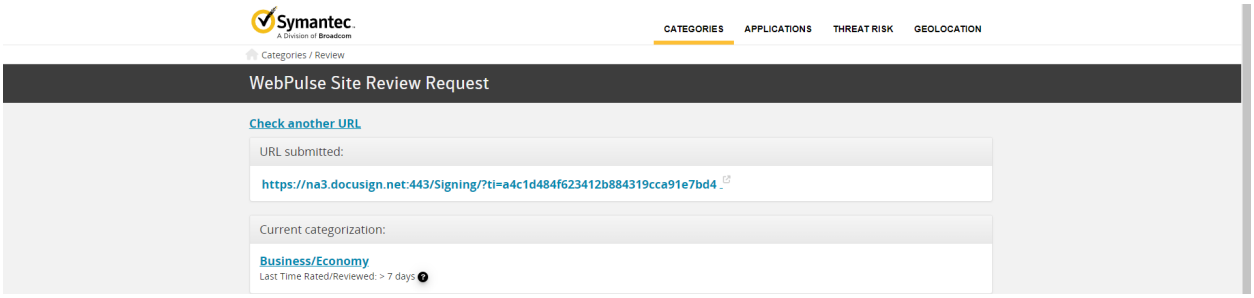


Zscaler Site Review

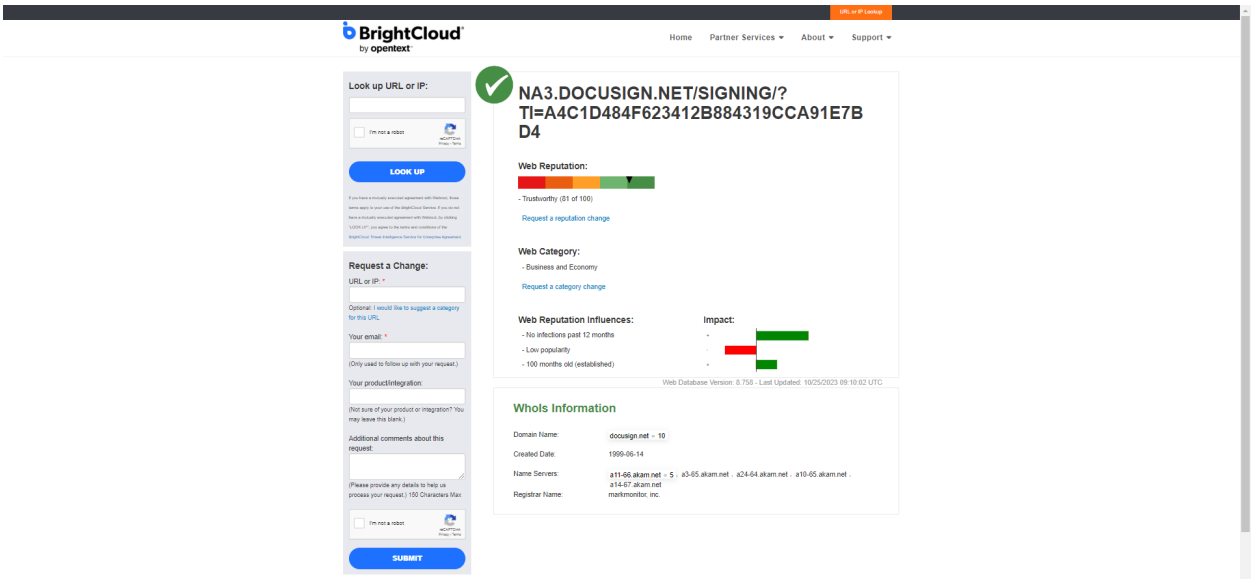
TCS Confidential


zscaler
Welcome to Site Review
With the URL Lookup tool you can find out how Zscaler categorizes a site (URL or IP Address) in its URL Filtering Database. Note that URL lookup results may vary from those seen in your environment due to possible custom categories that your admin might have configured.
Step 2. Request Review
URL
CURRENT CATEGORIES
SUGGESTED CATEGORIES
See definition of URL categories here
na3.docusign.net 5 /Signing/?ti=
a4c1d484f623412b884319cca91e7bd4
Professional Services
Select Categories

Symantec Site Review



BrightCloud



We have obderved below phishing URL in other emails sent by same sender with different subjects which prompts for email and password.

1) [https[:]//dftyhq.companyworkplacenow-setup.info/SAAKIvBX](https://dftyhq.companyworkplacenow-setup.info/SAAKIvBX)

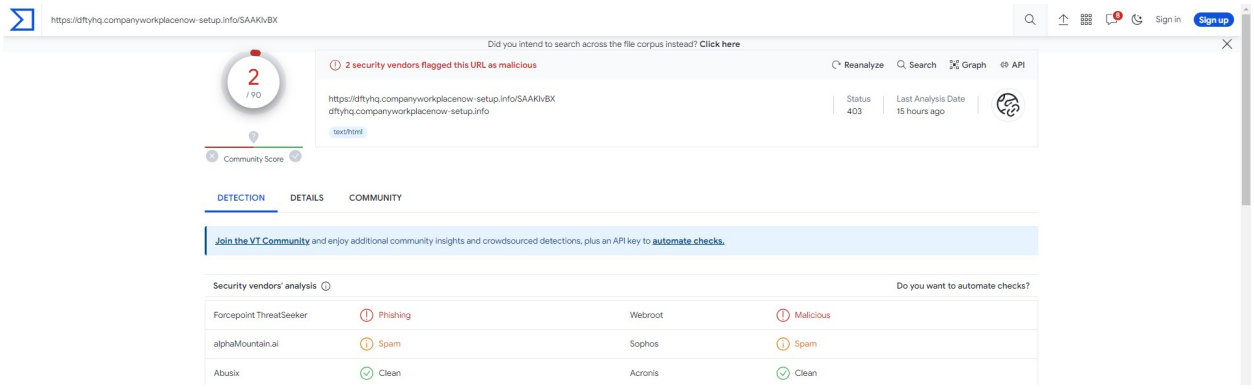
Reputation-Phishing

URL Hosted IP- 104[.]21[.]36[.]108

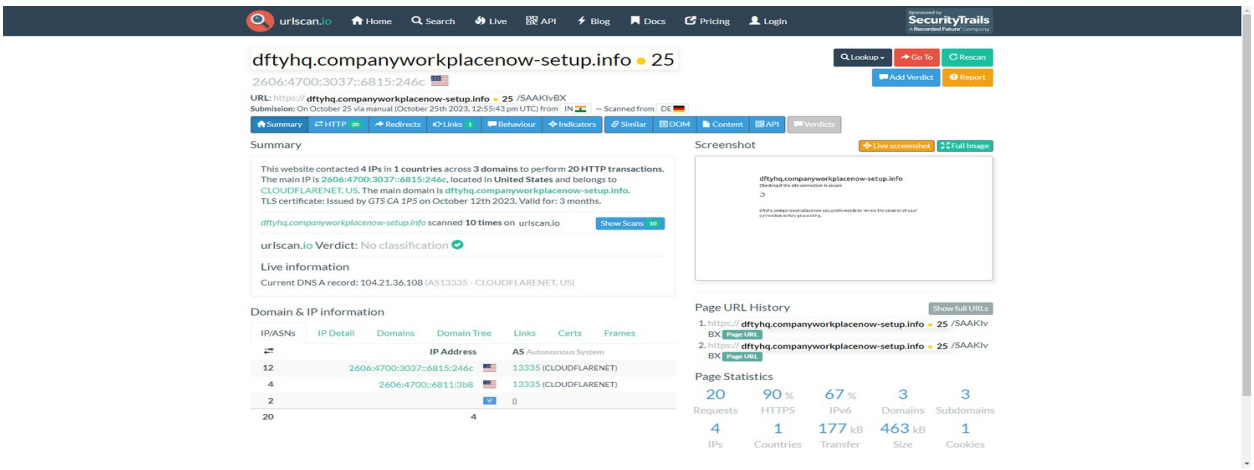
Verdict-**Malicious**

(VT-0, RF-26,IPVoid-0,AbuseIPDB-4 times with confidence 0%,BrightCloud-High Risk for Phishing and Proxy)

Virus Total

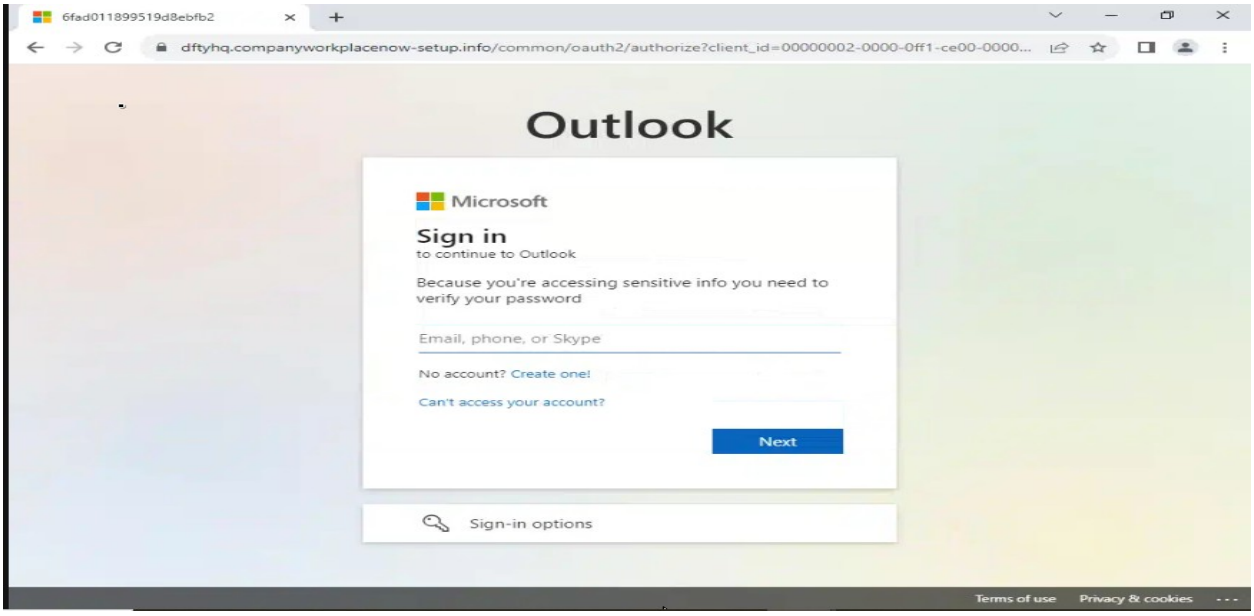


URLScanIO

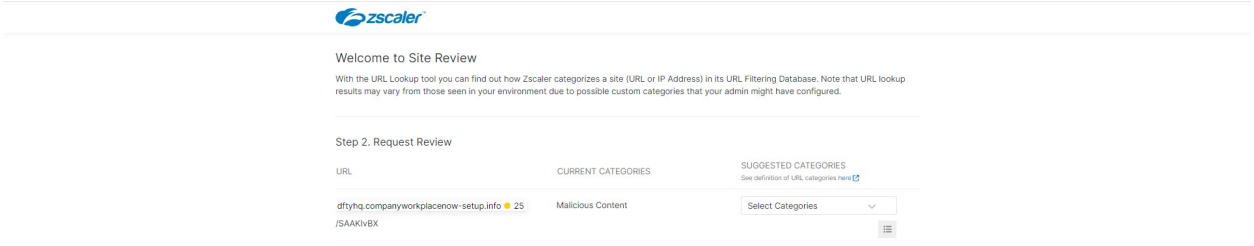


Browserling

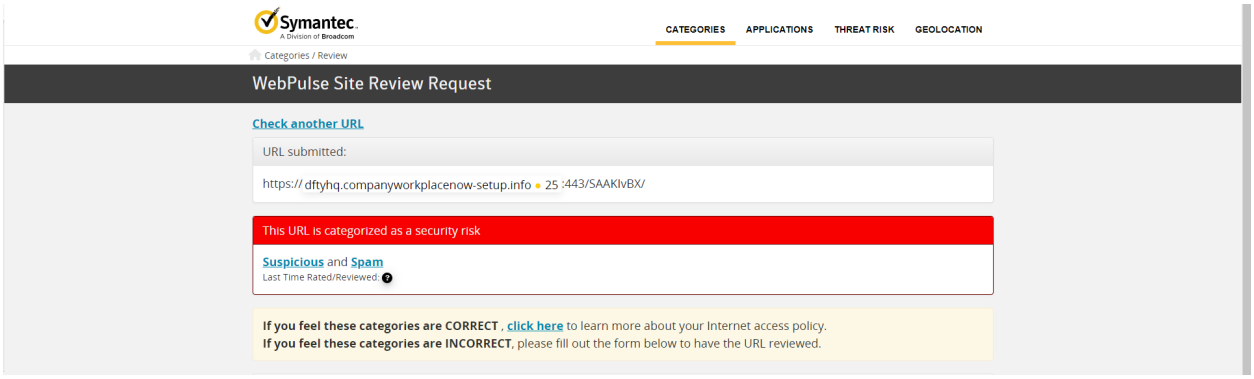
TCS Confidential



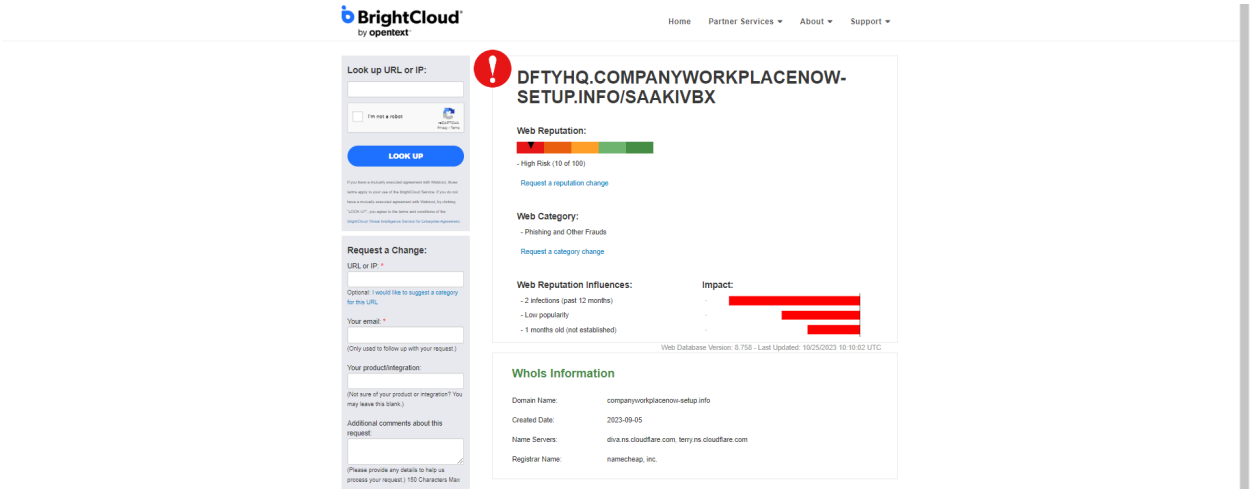
Zscaler Site Review


zscaler
Welcome to Site Review
With the URL Lookup tool you can find out how Zscaler categorizes a site (URL or IP Address) in its URL Filtering Database. Note that URL lookup results may vary from those seen in your environment due to possible custom categories that your admin might have configured.
Step 2. Request Review
URL
CURRENT CATEGORIES
SUGGESTED CATEGORIES
dftyhq.companyworkplacenow-setup.info 25
/SAAKIvBX
Malicious Content
Select Categories

Symantec Site Review


Symantec
A Division of Broadcom
CATEGORIES
APPLICATIONS
THREAT RISK
GEOLOCATION
Categories / Review
WebPulse Site Review Request
Check another URL
URL submitted:
https:// dftyhq.companyworkplacenow-setup.info 25 :443/SAAKIvBX/
This URL is categorized as a security risk
Suspicious and Spam
Last Time Rated/Reviewed:
If you feel these categories are CORRECT , click here to learn more about your Internet access policy.
If you feel these categories are INCORRECT, please fill out the form below to have the URL reviewed.

BrightCloud


BrightCloud
by opentext
Home
Partner Services
About
Support
Look up URL or IP:
I'm not a robot
LOOK UP
Request a Change:
URL or IP: *
Optional: I would like to suggest a category for this URL
Your email: *
(Only used to follow up with your request.)
Your product/integration:
(Not sure of your product or integration? You may leave this blank.)
Additional comments about this request:
(Please provide any details to help us process your request.) 150 Characters Max
DFTYHQ.COMPANYWORKPLACENOW-SETUP.INFO/SAAKIVBX
Web Reputation:
- High Risk (10 of 100)
Request a reputation change
Web Category:
- Phishing and Other Frauds
Request a category change
Web Reputation Influences:
Impact:
- 2 infections (past 12 months)
- Low popularity
- 1 months old (not established)
Web Database Version: 8.758 - Last Updated: 10/25/2023 10:10:02 UTC
Whois Information
Domain Name: companyworkplacenow-setup.info
Created Date: 2023-09-05
Name Servers: diva.ns.cloudflare.com, terry.ns.cloudflare.com
Registrar Name: namecheap, inc.

Attachment Analysis

There is no attachment present in email.

Email Log Analysis

Sender ID-Total-321 Delivered-23

Subject-Total-36 Delivered-19

Domain- Total-321 Delivered-23

❖ Identified IOCs

URL

1) https[:]//aquapham.net/viewer/?ur=email&dn=domain.com

2) https[:]//protect.docusign.net/report-abuse?e=AUtomjpFak9GlbPL0zFFi11rxo2a-L1l0xL9xVFfCnMLPrRH-kEUxclfSiIx1Rl9NoYynu2kl0PLTneyDgqvPh2kaLzX2GWMcrpnKa_WguA7j8YnLTm4mV3py6FKwyJw5neKuzTo2DTmkzV6c9_OH8-xZi62l_lAuyQRZUj6x-2EUuVAty5_wXCFE8HsIBnfETBp9I2jU-GWJrZLVQuN6Jgq0SPcPPIRPYAfuIMuS4xv_NNkOqZrjFo4WztXYDHz6BPCs2Vz4--Y3QsgJdRSpXeg7EL20XeC2PMks8JcSXjTthFEtZFlT-FJNUx8OwI5L7KbE2D4WmVvRkREz03STmh5RfAJFNTwP8XcZj8snRw_uQ7OEb_0JSg_wf8989LmbrrxVFLdVGaDaU_xnjkh65hXWaXxp6FfMWRphCrm18NFL5UqPYTV3q2pbw8-lFnjeX3O9SAUwoGSp0OJwJ9zf0B5FMLYGUCUsuDoCsr5ko_6&lang=en

3) https[:]//support.docusign.com/en/guides/Declining-to-sign-DocuSign-Signer-Guide

4) https[:]//support.docusign.com/en/articles/How-do-I-manage-my-email-notifications

5) https[:]//www.docusign.com/support

6) https[:]//support.docusign.com/articles/How-do-I-sign-a-DocuSign-document-Basic-Signing

7) https[:]//www.docusign.com/features-and-benefits/mobile

8) https[:]//na3.docusign.net/Signing/?ti=dc8afed6dd7f4ed49e7f6730c7343133

9) https[:]//dftyhq.companyworkplacenow-setup.info/SAAKIvBX

Domain

1. aquapham[.]net
2. Docusign[.]com
3. Dftyhq[.]companyworkplacenow-setup[.]info

Hashes

1. a109f90cc0133b07426751e60c695133c5bbbc439c7a27cee0c888cc25554bed

IP Address

1. 193[.]233[.]203[.]242
2. 210[.]122[.]9[.]62
3. 45[.]141[.]152[.]19
4. 64[.]207[.]218[.]159
5. 13[.]110[.]26[.]11
6. 13[.]110[.]26[.]13
7. 151[.]101[.]194[.]133
8. 151[.]101[.]130[.]133
9. 64[.]207[.]218[.]236
10. 104[.]21[.]36[.]108

Email

1. root@rhinestone-nailheads[.]com

Blocked Malicious IOCs

URL

1. https[:]//aquapham.net/viewer/?ur=email&dn=domain.com
2. https[:]//dftyhq.companyworkplacenow-setup.info/SAAKIvBX

Domain

1. aquapham[.]net
2. dftyhq[.]scompanyworkplacenow-setup[.]info

Hashes

1. a109f90cc0133b07426751e60c695133c5bbbc439c7a27cee0c888cc25554bed

IP Address

1. 45[.]141[.]152[.]19
2. 104[.]21[.]36[.]108

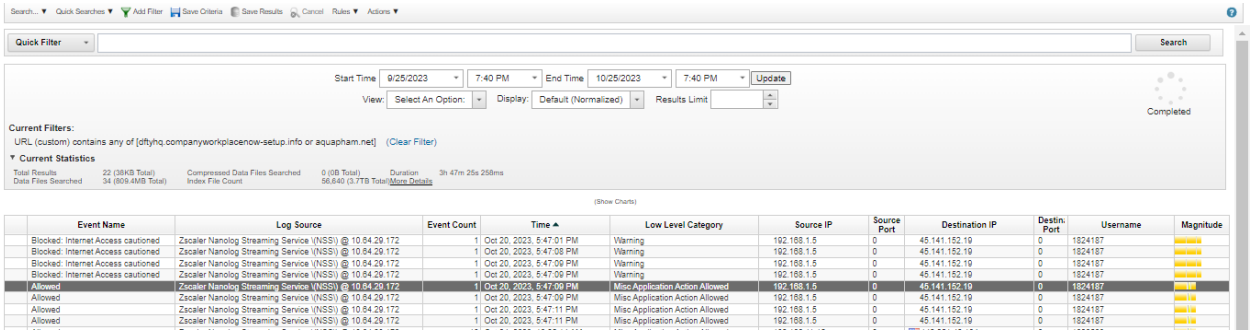
Email-

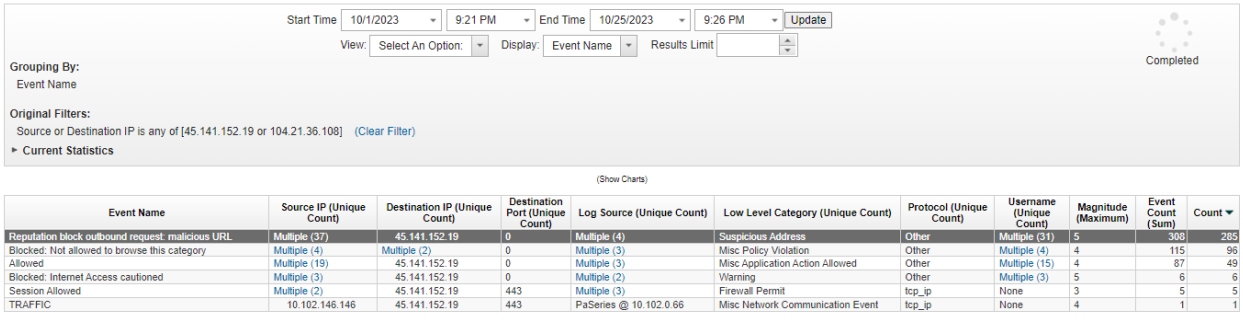
1. root@rhinestone-nailheads[.]com

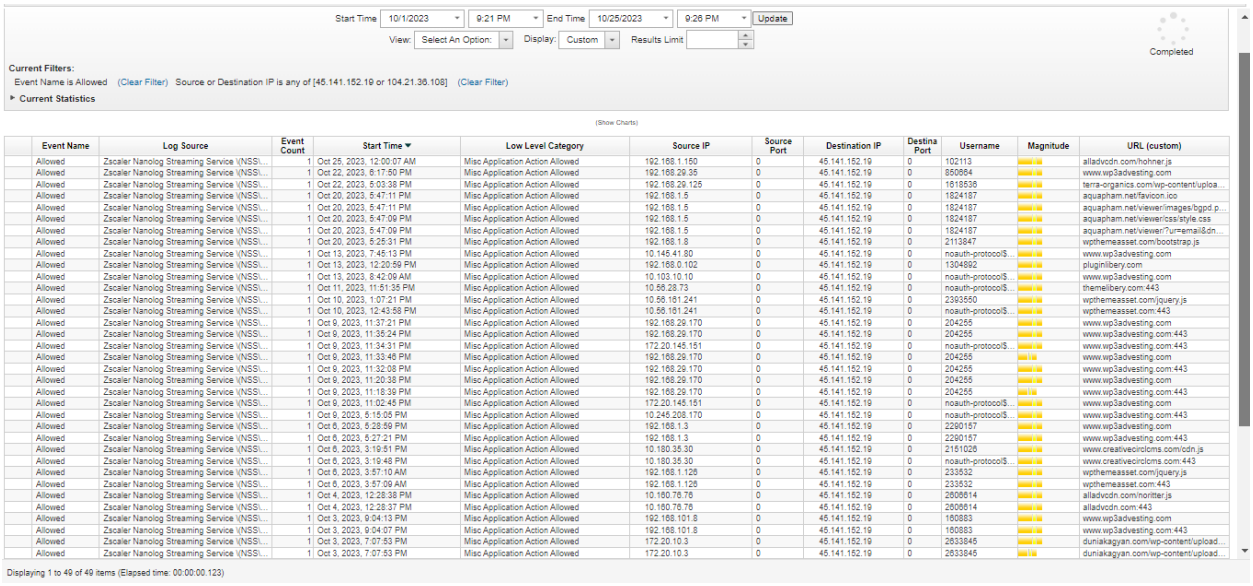
Communication to Phishing URLs.

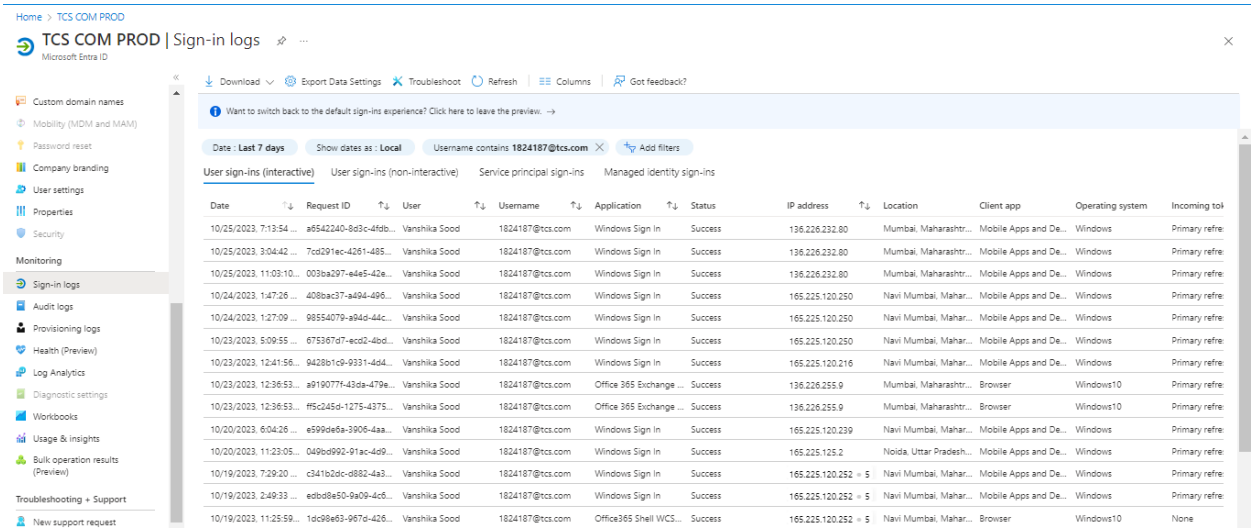
We have observed below associate has accessed phishing URL. We have not seen any suspicious activity from associate id.

Date/Time-Oct 20, 2023, 3:31:33 PM
User- 1824187@tcs.com
Hostname- 01HW1471208

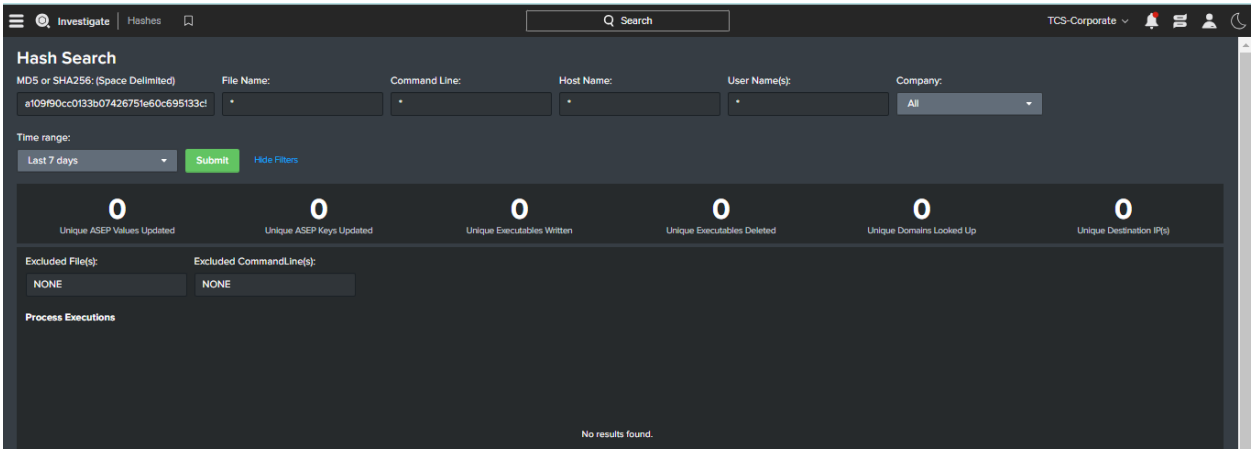

Quick Filter
Search
Start Time 9/25/2023 7:40 PM End Time 10/25/2023 7:40 PM Update
View: Select An Option: Display: Default (Normalized) Results Limit
Completed
Current Filters:
URL (custom) contains any of [dftyhq.companyworkplacenow-setup.info or aquapham.net] (Clear Filter)
Current Statistics
Total Results 22 (38KB Total) Compressed Data Files Searched 0 (0B Total) Duration 3h 47m 25s 258ms
Data Files Searched 34 (809.4MB Total) Index File Count 56,640 (3.7TB Total) More Details
(Show Charts)
Event Name | Log Source | Event Count | Time | Low Level Category | Source IP | Source Port | Destination IP | Destin. Port | Username | Magnitude
Blocked: Internet Access cautioned | Zscaler Nanolog Streaming Service \(NSS\) @ 10.84.29.172 | 1 | Oct 20, 2023, 5:47:01 PM | Warning | 192.168.1.5 | 0 | 45.141.152.19 | 0 | 1824187
Blocked: Internet Access cautioned | Zscaler Nanolog Streaming Service \(NSS\) @ 10.84.29.172 | 1 | Oct 20, 2023, 5:47:08 PM | Warning | 192.168.1.5 | 0 | 45.141.152.19 | 0 | 1824187
Blocked: Internet Access cautioned | Zscaler Nanolog Streaming Service \(NSS\) @ 10.84.29.172 | 1 | Oct 20, 2023, 5:47:09 PM | Warning | 192.168.1.5 | 0 | 45.141.152.19 | 0 | 1824187
Blocked: Internet Access cautioned | Zscaler Nanolog Streaming Service \(NSS\) @ 10.84.29.172 | 1 | Oct 20, 2023, 5:47:09 PM | Warning | 192.168.1.5 | 0 | 45.141.152.19 | 0 | 1824187
Allowed | Zscaler Nanolog Streaming Service \(NSS\) @ 10.84.29.172 | 1 | Oct 20, 2023, 5:47:09 PM | Misc Application Action Allowed | 192.168.1.5 | 0 | 45.141.152.19 | 0 | 1824187
Allowed | Zscaler Nanolog Streaming Service \(NSS\) @ 10.84.29.172 | 1 | Oct 20, 2023, 5:47:09 PM | Misc Application Action Allowed | 192.168.1.5 | 0 | 45.141.152.19 | 0 | 1824187
Allowed | Zscaler Nanolog Streaming Service \(NSS\) @ 10.84.29.172 | 1 | Oct 20, 2023, 5:47:11 PM | Misc Application Action Allowed | 192.168.1.5 | 0 | 45.141.152.19 | 0 | 1824187
Allowed | Zscaler Nanolog Streaming Service \(NSS\) @ 10.84.29.172 | 1 | Oct 20, 2023, 5:47:11 PM | Misc Application Action Allowed | 192.168.1.5 | 0 | 45.141.152.19 | 0 | 1824187


Start Time 10/1/2023 9:21 PM End Time 10/25/2023 9:26 PM Update
View: Select An Option: Display: Event Name Results Limit
Completed
Grouping By:
Event Name
Original Filters:
Source or Destination IP is any of [45.141.152.19 or 104.21.36.108] (Clear Filter)
Current Statistics
(Show Charts)
Event Name | Source IP (Unique Count) | Destination IP (Unique Count) | Destination Port (Unique Count) | Log Source (Unique Count) | Low Level Category (Unique Count) | Protocol (Unique Count) | Username (Unique Count) | Magnitude (Maximum) | Event Count (Sum) | Count
Reputation block outbound request: malicious URL | Multiple (37) | 45.141.152.19 | 0 | Multiple (4) | Suspicious Address | Other | Multiple (31) | 5 | 308 | 285
Blocked: Not allowed to browse this category | Multiple (4) | Multiple (2) | 0 | Multiple (3) | Misc Policy Violation | Other | Multiple (4) | 4 | 115 | 96
Allowed | Multiple (19) | 45.141.152.19 | 0 | Multiple (3) | Misc Application Action Allowed | Other | Multiple (15) | 4 | 87 | 49
Blocked: Internet Access cautioned | Multiple (3) | 45.141.152.19 | 0 | Multiple (2) | Warning | Other | Multiple (3) | 5 | 6 | 6
Session Allowed | Multiple (2) | 45.141.152.19 | 443 | Multiple (3) | Firewall Permit | tcp_ip | None | 3 | 5 | 5
TRAFFIC | 10.102.146.146 | 45.141.152.19 | 443 | PaSeries @ 10.102.0.66 | Misc Network Communication Event | tcp_ip | None | 4 | 1 | 1


Start Time 10/1/2023 9:21 PM End Time 10/25/2023 9:26 PM Update
View: Select An Option: Display: Custom Results Limit
Completed
Current Filters:
Event Name is Allowed (Clear Filter) Source or Destination IP is any of [45.141.152.19 or 104.21.36.108] (Clear Filter)
Current Statistics
(Show Charts)
Event Name | Log Source | Event Count | Start Time | Low Level Category | Source IP | Source Port | Destination IP | Destina Port | Username | Magnitude | URL (custom)
Displaying 1 to 49 of 49 items (Elapsed time: 00:00:00.123)


Home > TCS COM PROD
TCS COM PROD | Sign-in logs
Microsoft Entra ID
Download Export Data Settings Troubleshoot Refresh Columns Got feedback?
Want to switch back to the default sign-ins experience? Click here to leave the preview.
Date : Last 7 days Show dates as : Local Username contains 1824187@tcs.com Add filters
User sign-ins (interactive) User sign-ins (non-interactive) Service principal sign-ins Managed identity sign-ins
Custom domain names
Mobility (MDM and MAM)
Password reset
Company branding
User settings
Properties
Security
Monitoring
Sign-in logs
Audit logs
Provisioning logs
Health (Preview)
Log Analytics
Diagnostic settings
Workbooks
Usage & insights
Bulk operation results (Preview)
Troubleshooting + Support
New support request

Hash Search



TCS Confidential

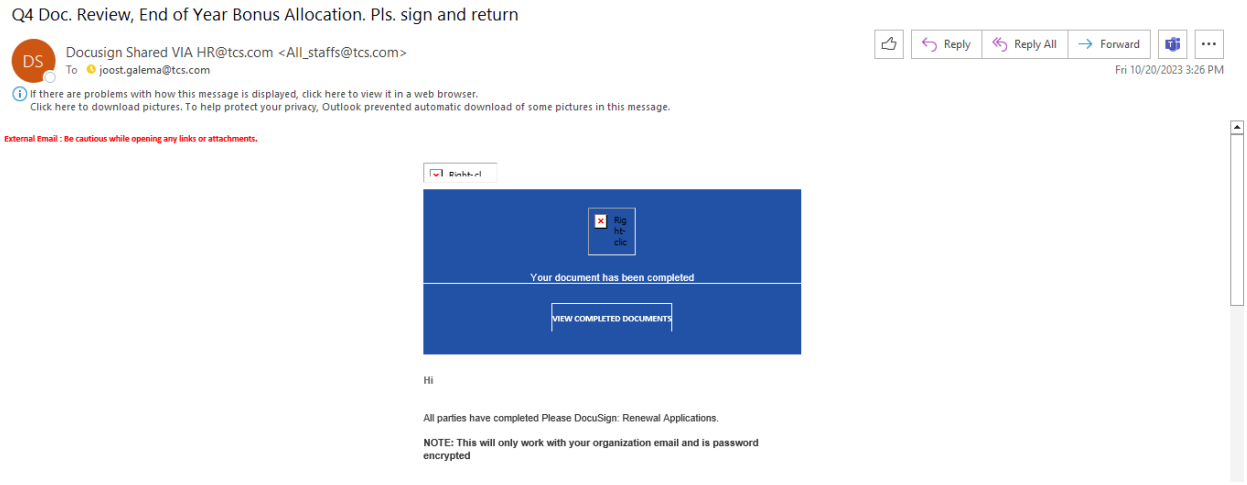
IMT Details

We have raised IMT for the incident-- ES191239.

Miscellaneous Observation

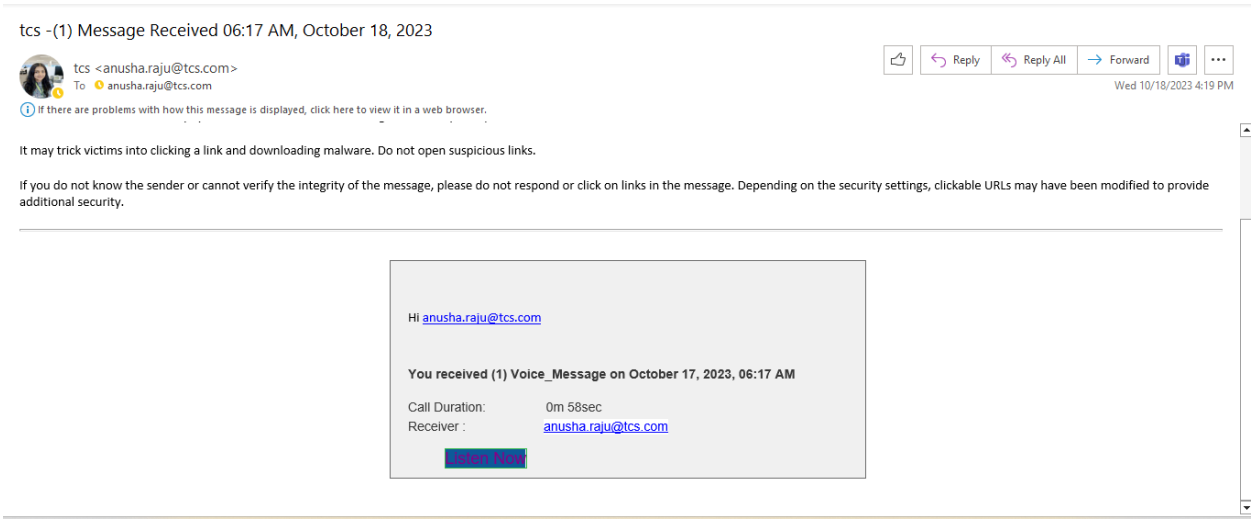
Emails Screenshots-

1.Q4 Doc. Review, End of Year Bonus Allocation. Pls. sign and return

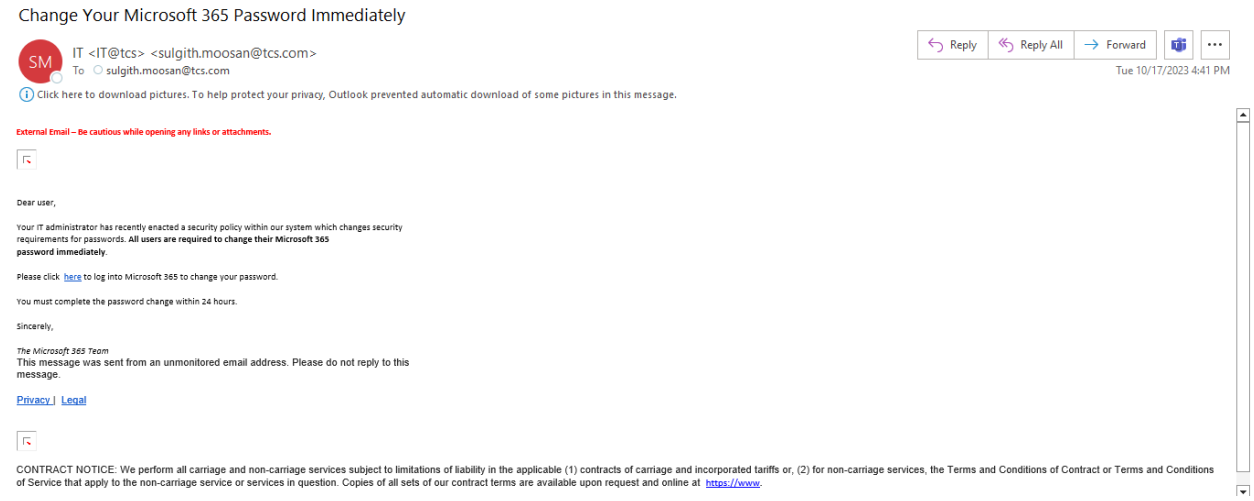

Q4 Doc. Review, End of Year Bonus Allocation. Pls. sign and return
DS
Docusign Shared VIA HR@tcs.com <All_staffs@tcs.com>
To joost.galema@tcs.com
Reply
Reply All
Forward
Fri 10/20/2023 3:26 PM
If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.
External Email : Be cautious while opening any links or attachments.
Your document has been completed
VIEW COMPLETED DOCUMENTS
Hi
All parties have completed Please DocuSign: Renewal Applications.
NOTE: This will only work with your organization email and is password encrypted

2.FYI

3.tcs -(1) Message Received 06:17 AM, October 18, 2023


tcs -(1) Message Received 06:17 AM, October 18, 2023
tcs <anusha.raju@tcs.com>
To anusha.raju@tcs.com
Reply
Reply All
Forward
Wed 10/18/2023 4:19 PM
If there are problems with how this message is displayed, click here to view it in a web browser.
It may trick victims into clicking a link and downloading malware. Do not open suspicious links.
If you do not know the sender or cannot verify the integrity of the message, please do not respond or click on links in the message. Depending on the security settings, clickable URLs may have been modified to provide additional security.
Hi anusha.raju@tcs.com
You received (1) Voice_Message on October 17, 2023, 06:17 AM
Call Duration: 0m 58sec
Receiver : anusha.raju@tcs.com
Listen Now

4.Change Your Microsoft 365 Password Immediately


Change Your Microsoft 365 Password Immediately
SM
IT <IT@tcs> <sulgith.moosan@tcs.com>
To sulgith.moosan@tcs.com
Reply
Reply All
Forward
Tue 10/17/2023 4:41 PM
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.
External Email – Be cautious while opening any links or attachments.
Dear user,
Your IT administrator has recently enacted a security policy within our system which changes security requirements for passwords. All users are required to change their Microsoft 365 password immediately.
Please click here to log into Microsoft 365 to change your password.
You must complete the password change within 24 hours.
Sincerely,
The Microsoft 365 Team
This message was sent from an unmonitored email address. Please do not reply to this message.
Privacy | Legal
CONTRACT NOTICE: We perform all carriage and non-carriage services subject to limitations of liability in the applicable (1) contracts of carriage and incorporated tariffs or, (2) for non-carriage services, the Terms and Conditions of Contract or Terms and Conditions of Service that apply to the non-carriage service or services in question. Copies of all sets of our contract terms are available upon request and online at https://www.